# Symantec™ Data Loss Prevention Administration Guide

Version 12.5



# Symantec Data Loss Prevention Administration Guide

Documentation version: 12.5a

### Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation 350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

# **Technical Support**

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

#### www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

### **Contacting Technical Support**

Customers with a current support agreement may access Technical Support information at the following URL:

#### www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

### Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

#### Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan customercare\_apac@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

# Contents

Technical Sup	pport	4
Section 1	Getting started	46
Chapter 1	Introducing Symantec Data Loss Prevention	47
	About Symantec Data Loss Prevention About the Enforce platform About Network Monitor and Prevent About Network Discover About Network Protect About Mobile Prevent About Mobile Email Monitor About Endpoint Discover About Endpoint Prevent	50 51 52 53 53
Chapter 2	Getting started administering Symantec Data Loss Prevention	55
	About Symantec Data Loss Prevention administration  About the Enforce Server administration console  Logging on and off the Enforce Server administration console  About the administrator account  Performing initial setup tasks  Changing the administrator password  Adding an administrator email account  Editing a user profile  Changing your password	56 57 58 58 59 60
Chapter 3	Working with languages and locales  About support for character sets, languages, and locales  Supported languages for detection  Working with international characters  About Symantec Data Loss Prevention language packs  About locales	64 65 67

	Using a non-English language on the Enforce Server administration console	
Section 2	Managing the Enforce Server platform	75
Chapter 4	Managing Enforce Server services and settings	
	About Data Lost Prevention services	
	Starting an Enforce Server on Windows	
	Stopping an Enforce Server on Windows	
	Starting a Detection Server on Windows	
	Stopping a Detection Server on Windows	
	Starting services on single-tier Windows installations	
	Stopping services on single-tier Windows installations	
	Starting and stopping services on Linux	
	Starting an Enforce Server on Linux	
	Stopping an Enforce Server on Linux	81
	Starting a detection server on Linux	
	Stopping a detection server on Linux	
	Starting services on single-tier Linux installations	
	Stopping services on single-tier Linux installations	83
Chapter 5	Managing roles and users	84
	About role-based access control	84
	About authenticating users	85
	About configuring roles and users	
	About recommended roles for your organization	
	Roles included with solution packs	
	Configuring roles	
	Configuring user accounts	
	Configuring password enforcement settings	
	Resetting the Administrator password	
	Manage and add roles	
	Manage and add users	
	Integrating Active Directory for user authentication	
	Creating the configuration file for Active Directory integration  Verifying the Active Directory connection	
	Configuring the Enforce Server for Active Directory	100
	authentication	109

	About configuring certificate authentication	110
	Configuring certificate authentication for the Enforce Server	440
	administration console	112
	Adding certificate authority (CA) certificates to the Tomcat trust store	114
	Mapping Common Name (CN) values to Symantec Data Loss	114
	Prevention user accounts	117
	About certificate revocation checks	
	Troubleshooting certificate authentication	
	Disabling password authentication and forms-based log on	
Chapter 6	Connecting to group directories	126
	Creating connections to LDAP servers	126
	Configuring directory server connections	
	Scheduling directory server indexing	
Chapter 7	Managing stored credentials	131
	About the credential store	131
	Adding new credentials to the credential store	
	Configuring endpoint credentials	
	Managing credentials in the credential store	133
Chapter 8	Managing system events and messages	134
	About system events	134
	System events reports	
	Working with saved system reports	
	Server event detail	139
	Configuring event thresholds and triggers	140
	About system event responses	142
	Enabling a syslog server	144
	About system alerts	146
	Configuring the Enforce Server to send email alerts	146
	Configuring system alerts	
	About log review	149
	System event codes and messages	150
Chapter 9	Adding a new product module	173
	Installing a new license file	173
	About system upgrades	174

Section 3	Managing detection servers	175
Chapter 10	Installing and managing detection servers	176
	About managing Symantec Data Loss Prevention servers  Enabling Advanced Process Control	
	Server controls	
	Server configuration—basic	
	Network Monitor Server—basic configuration	
	Network Prevent for Email Server—basic configuration	184
	Network Prevent for Web Server—basic configuration	187
	Network Discover Server and Network Protect—basic configuration	190
	Endpoint Server—basic configuration	
	Classification Server—basic configuration	
	Server configuration—advanced	
	Adding a detection server	194
	Removing a server	196
	Importing SSL certificates to Enforce or Discover servers	197
	About the System Overview screen	198
	Server status overview	
	Recent error and warning events list	
	Server Detail screen	
	Advanced server settings	
	About using load balancers in an endpoint deployment	240
Chapter 11	Managing log files	243
	About log files	243
	Operational log files	
	Debug log files	247
	Log collection and configuration screen	252
	Configuring server logging behavior	252
	Collecting server logs and configuration files	257
	About log event codes	261
	Network and Mobile Prevent for Web operational log files and event codes	262
	Network and Mobile Prevent for Web access log files and fields	264
	Network and Mobile Prevent for Web protocol debug log	
	files	
	Network Prevent for Email log levels	
	Network Prevent for Email operational log codes	267

	Network Prevent for Email originated responses and codes	271
Chapter 12	Using Symantec Data Loss Prevention utilities	274
	About the Symantec Data Loss Prevention utilities	274
	About Endpoint utilities	
	About the Environment Check Utility	
	Running the Environment Check Utility on Windows	
	Running the Environment Check Utility on Linux	
	About Environment Check Utility output	278
	About DBPasswordChanger	279
	DBPasswordChanger syntax	279
	Example of using DBPasswordChanger	279
Section 4	Authoring policies	281
Chapter 13	Introduction to policies	283
	About Data Loss Prevention policies	283
	Policy components	
	Policy templates	
	Solution packs	
	Policy groups	
	Policy deployment	
	Policy severity	289
	Policy authoring privileges	290
	Data Profiles	291
	User Groups	292
	Policy import and export	292
	Workflow for implementing policies	
	Viewing, printing, and downloading policy details	295
Chapter 14	Overview of policy detection	296
	Detecting data loss	296
	Content that can be detected	297
	Files that can be detected	297
	Protocols that can be monitored	297
	Endpoint events that can be detected	298
	Identities that can be detected	
	Languages that can be detected	
	Data Loss Prevention policy detection technologies	
	Policy matching conditions	
	Content matching conditions	301

	File property matching conditions  Protocol matching condition for network and mobile	303
	Endpoint matching conditions	
	Groups (identity) matching conditions	
	Detection messages and message components	
	Exception conditions	
	Compound conditions	308
	Policy detection execution	308
	Two-tier detection for DLP Agents	309
Chapter 15	Creating policies from templates	312
	Creating a policy from a template	312
	US Regulatory Enforcement policy templates	315
	UK and International Regulatory Enforcement policy templates	317
	Customer and Employee Data Protection policy templates	317
	Confidential or Classified Data Protection policy templates	319
	Network Security Enforcement policy templates	320
	Acceptable Use Enforcement policy templates	320
	Choosing an Exact Data Profile	322
	Choosing an Indexed Document Profile	323
Chapter 16	Configuring policies	325
	Adding a new policy or policy template	325
	Configuring policies	326
	Adding a rule to a policy	328
	Configuring policy rules	330
	Defining rule severity	333
	Configuring match counting	334
	Selecting components to match on	336
	Adding an exception to a policy	
	Configuring policy exceptions	
	Configuring compound match conditions	
	Input character limits for policy configuration	
Chapter 17	Administering policies	345
	Manage and add policies	345
	Manage and add policy groups	
	Creating and modifying policy groups	
	Importing policy templates	
	Exporting policy detection as a template	
		350

	Removing policies and policy groups	351
	Viewing and printing policy details	
	Downloading policy details	
	Troubleshooting policies	
	Updating EDM and IDM profiles to the latest version	354
	Updating policies after upgrading to the latest version	
Chapter 18	Best practices for authoring policies	357
	Best practices for authoring policies  Develop a policy strategy that supports your data security	
	objectives	
	Use a limited number of policies to get started	
	Use policy templates but modify them to meet your requirements Use the appropriate match condition for your data loss prevention	360
	objectives	360
	Test and tune policies to improve match accuracy	361
	Start with high match thresholds to reduce false positives	362
	Use a limited number of exceptions to narrow detection scope	
	Use compound conditions to improve match accuracy	363
	Author policies to limit the potential effect of two-tier detection	364
	Use policy groups to manage policy lifecycle	365
	Follow detection-specific best practices	365
Chapter 19	Detecting content using Exact Data Matching	
	(EDM)	367
	Introducing Exact Data Matching (EDM)	367
	About using EDM to protect content	
	EDM policy features	369
	EDM policy templates	370
	About the Exact Data Profile and index	371
	About the exact data source file	372
	About cleansing the exact data source file	373
	About using System Fields for data source validation	374
	About index scheduling	
	About the Content Matches Exact Data From condition	375
	About Data Owner Exception	375
	About profiled Directory Group Matching (DGM)	376
	About two-tier detection for EDM on the endpoint	377
	About upgrading EDM deployments	377
	Configuring Exact Data profiles	378
	Creating the exact data source file for EDM	379

Creating the exact data source file for Data Owner	
Exception	380
Creating the exact data source file for profiled DGM	380
Preparing the exact data source file for indexing	
Uploading exact data source files to the Enforce Server	383
Creating and modifying Exact Data Profiles	385
Mapping Exact Data Profile fields	389
Using system-provided pattern validators for EDM profiles	391
Scheduling Exact Data Profile indexing	392
Managing and adding Exact Data Profiles	394
Configuring EDM policies	395
Configuring the Content Matches Exact Data policy	
condition	396
Configuring Data Owner Exception for EDM policy	
conditions	398
Configuring the Sender/User based on a Profiled Directory policy	
condition	399
Configuring the Recipient based on a Profiled Directory policy	
condition	
Configuring Advanced Server Settings for EDM policies	400
Using multi-token matching	403
Characteristics of multi-token cells	
Multi-token with spaces	
Multi-token with stopwords	405
Multi-token with mixed language characters	405
Multi-token with punctuation	
Additional examples for multi-token cells with punctuation	407
Some special use cases for system-recognized data	
patterns	
Multi-token punctuation characters	
Match count variant examples	
Proximity matching example	
Updating EDM indexes to version 12.5	
Update process using the Remote EDM Indexer	
Update process using the Enforce Server	
EDM index out of date error codes	
Memory requirements for EDM	
Multi-token memory table	
EDM index size table	424
Determining how much memory is needed to index the data	
source	424
Determining how much memory is needed to load the index into	
memory on the detection server	426

Determining and setting the memory for the detection server	427
Increasing the memory for the Enforce Server EDM indexer	429
Increasing the memory for the Remote EDM indexer	429
Increasing the memory for the detection server (File	
Reader)	430
Additional example memory requirement calculations	431
Remote EDM indexing	432
About the Remote EDM Indexer	433
About the SQL Preindexer	433
System requirements for remote EDM indexing	434
Workflow for remote EDM indexing	434
About installing and running the Remote EDM Indexer and SQL	
Preindexer utilities	435
Creating an EDM profile template for remote indexing	436
Downloading and copying the EDM profile file to a remote	
system	439
Generating remote index files	
Remote indexing examples using data source file	440
Remote indexing examples using SQL Preindexer	
Copying and loading remote index files to the Enforce	
Server	442
SQL Preindexer command options	443
Remote EDM Indexer command options	445
Troubleshooting preindexing errors	
Troubleshooting remote indexing errors	
Installing the Remote EDM Indexer (Windows)	
Installing the Remote EDM Indexer (Linux)	
Best practices for using EDM	
Ensure data source has at least one column of unique data	
Cleanse the data source file of blank columns and duplicate	
rows	453
Remove ambiguous character types from the data source	
file	454
Understand how multi-token cell matching functions	
Do not use the comma delimiter if the data source has number	
fields	455
Map data source column to system fields to leverage	
validation	455
Ensure that the data source is clean for indexing	
Leverage EDM policy templates when possible	
Include column headers as the first row of the data source	
file	456
Check the system alerts to tune profile accuracy	

	Use stopwords to exclude common words from detection	
	Use scheduled indexing to automate profile updates	457
	Match on 3 columns in an EDM condition to increase detection	450
	accuracy	
	Leverage exception tuples to avoid false positives	459
	Use a WHERE clause to detect records that meet specific	400
	criteria	
	Use the minimum matches field to fine tune EDM rules	460
	Combine Data Identifiers with EDM rules to limit the impact of	400
	two-tier detection	460
	Include an email address field in the Exact Data Profile for profiled  DGM	461
	Use profiled DGM for Network Prevent for Web identity	404
	detection	401
Chapter 20	Datacting contant using Indoved Document	
chapter 20	Detecting content using Indexed Document	
	Matching (IDM)	462
	Introducing Indexed Document Matching (IDM)	462
	About using IDM	
	Supported forms of matching for IDM	
	Types of IDM detection	
	About the Indexed Document Profile	
	About the document data source	
	About the indexing process	
	About indexing remote documents	
	About the server and agent index files	
	About index deployment and logging	
	Using IDM to detect exact files	
	Using IDM to detect exact and partial file contents	
	About using the Content Matches Document Signature policy	
	condition	473
	About using IDM for policy exceptions	
	About whitelisting partial file contents	
	Configuring IDM profiles and policy conditions	
	Preparing the document data source for indexing	
	Whitelisting file contents to exclude from partial matching	
	Manage and add Indexed Document Profiles	
	Creating and modifying Indexed Document Profiles	
	Uploading a document archive to the Enforce Server	
	Referencing a document archive on the Enforce Server	
	Using local path on Enforce Server	
	Using the remote SMB share option to index file shares	
	osing the remote own share option to index the shares	+00

	Using the remote SMB share option to index SharePoint	
	documents	487
	Filtering documents by file name	489
	Filtering documents by file size	491
	Scheduling document profile indexing	492
	Changing the default indexer properties	493
	Using agent IDM after upgrade to version 12.5	494
	Enabling agent IDM	495
	Estimating endpoint memory use for agent IDM	496
	Configuring the Content Matches Document Signature policy condition	497
	Best practices for using IDM	
	Reindex IDM profiles after major upgrade	
	Do not compress files in the document source	
	Avoid using IDM solely for binary files	
	Do not index empty documents	
	Prefer exact match over two-tier detection on the endpoint	
	Understand limitations of exact matching	
	Use whitelisting to exclude non-sensitive content from partial	002
	matching	503
	Filter documents from indexing to reduce false positives	
	Distinguish IDM exceptions from whitelisting and filtering	
	Create separate profiles to index large document sources	
	Use WebDAV or CIFS to index remote document data	
	sources	
	Use scheduled indexing to keep profiles up to date	
	Use parallel IDM rules to tune match thresholds	
	Use agent IDM with VML for partial match validation	507
Chapter 21	Detecting content using Vector Machine Learning	
	(VML)	509
	Introducing Vector Machine Learning (VML)	509
	About the Vector Machine Learning Profile	
	About the content you train	
	About the base accuracy from training percentage rates	
	About the Similarity Threshold and Similarity Score	
	About using unaccepted VML profiles in policies	
	Configuring VML profiles and policy conditions	
	Creating new VML profiles	
	Working with the Current Profile and Temporary Workspace	
	tabs	
	Uploading example documents for training	516

	Training VML profiles	518
	Adjusting memory allocation	520
	Managing training set documents	521
	Managing VML profiles	522
	Changing names and descriptions for VML profiles	524
	Configuring the Detect using Vector Machine Learning Profile	
	condition	525
	Configuring VML policy exceptions	526
	Adjusting the Similarity Threshold	527
	Testing and tuning VML profiles	
	Properties for configuring training	529
	Log files for troubleshooting VML training and policy	=0.4
	detection	
	Best practices for using VML	
	When to use VML	
	When not to use VML	
	Recommendations for training set definition	
	Guidelines for training set sizing	
	Recommendations for uploading documents for training	
	Guidelines for profile sizing	
	Recommendations for accepting or rejecting a profile	
	Guidelines for accepting or rejecting training results	
	Recommendations for deploying profiles	540
Chapter 22	Detecting content using data identifiers	541
	Introducing data identifiers	E11
	System-defined data identifiers	
	Extending and customizing data identifiers	
	About data identifier configuration	
	About data identifier breadths	
	About optional validators for data identifiers	
	About data identifier patterns	
	About pattern validators	
	About data normalizers	
	About cross-component matching	
	About unique match counting	
	Conifuring data identifier policy conditions	
	Workflow for configuring data identifier policies	
	Managing and adding data identifiers	
	Editing data identifiers	
	Configuring the Content Matches data identifier condition	
	Using data identifier breadths	554

	Selecting a data identifier breadth	555
	Using optional validators	558
	Configuring optional validators	559
	Acceptable characters for optional validators	560
	Using unique match counting	562
	Configuring unique match counting	563
	Modifying system data identifiers	564
	Cloning a system data identifier before modifying it	565
	Editing pattern validator input	566
	List of pattern validators that accept input data	566
	Editing keywords for international PII data identifiers	567
	List of keywords for international system data identifiers	568
	Updating policies to use the Randomized US SSN data	
	identifier	569
	Creating custom data identifiers	570
	Workflow for creating custom data identifiers	570
	Custom data identifier configuration	572
	Using the data identifier pattern language	573
	Writing data identifier patterns to match data	
	Using pattern validators	575
	Selecting pattern validators	577
	Selecting a data normalizer	578
	Creating custom script validators	579
	Best practices for using data identifiers	579
	Use data identifiers instead of regular expressions to improve accuracy	E90
	•	360
	Clone system-defined data identifiers before modifying to preserve	E01
	original state	301
	Modify data identifier definitions when you want tuning to apply	E04
	globally	301
	Consider using multiple breadths in parallel to detect different	E00
	severities of confidential data	302
	Avoid matching on the Envelope over HTTP to reduce false	E00
	positives	
	Use the Randomized US SSN data identifier to detect SSNs	582
	Use unique match counting to improve accuracy and ease	E00
	remediation	ებპ
Chapter 23	Detecting content using keyword matching	584
	Introducing keyword matching	584
	About keyword matching for Chinese, Japanese, and Korean	
	(CJK) languages	585
	\ , - JJ	

	About keyword proximity	586
	Keyword matching syntax	586
	Keyword matching examples	587
	Keyword matching examples for CJK languages	588
	About updates to the Drug, Disease, and Treatment keyword	
	lists	589
	Configuring keyword matching	590
	Configuring the Content Matches Keyword condition	591
	Enabling and using CJK token verification for server keyword	
	matching	593
	Updating the Drug, Disease, and Treatment keyword lists for your	
	HIPAA and Caldicott policies	594
	Best practices for using keyword matching	595
	Enable token verification on the server to reduce false positives	
	for CJK keyword detection	596
	Keep the keyword lists for your HIPAA and Caldicott policies up	
	to date	596
	Tune keywords lists for data identifiers to improve match	
	accuracy	597
	Use keyword matching to detect document metadata	
	Use VML to generate and maintain large keyword	
	dictionaries	597
Chapter 24	Detecting content using regular expressions	598
	Introducing regular expression matching	598
	About writing regular expressions	
	Configuring the Content Matches Regular Expression condition	
	Best practices for using regular expression matching	
	When to use regular expression matching	
	Use look ahead and look behind characters to improve regex	
	accuracy	602
	Use regular expressions sparingly to support efficient	
	performance	603
	Test regular expressions before deployment to improve	
	accuracy	603
	•	
Chapter 25	Detecting international language content	604
	Detecting non-English language content	604
	Best practices for detecting non-English language content	
	Upgrade to the latest version of Data Loss Prevention	
	Use international policy templates for policy creation	
	Use custom keywords for system data identifiers	

	Enable token validation to match Chinese, Japanese, and Korean keywords on the server	608
Chapter 26	Detecting file properties	609
	Introducing file property detection	609
	About file type matching	609
	About file format support for file type matching	610
	About custom file type identification	610
	About file size matching	611
	About file name matching	611
	Configuring file property matching	611
	Configuring the Message Attachment or File Type Match condition	. 612
	Configuring the Message Attachment or File Size Match	
	condition	613
	Configuring the Message Attachment or File Name Match condition	611
	File name matching syntax	
	File name matching examples	
	Enabling the Custom File Type Signature condition in the policy	013
	console	616
	Configuring the Custom File Type Signature condition	
	Best practices for using file property matching	
	Use compound file property rules to protect design and multimedia	010
	files	. 618
	Do not use file type matching to detect content	
	Calculate file size properly to improve match accuracy	
	Use expression patterns to match file names	
	Use scripts and plugins to detect custom file types	
Chapter 27	Detecting email for data classification services	620
	About implementing detection for Enterprise Vault Classification About matching on the message Subject for Data Classification	
	Services	
	Enabling classification test mode	621
	condition	623
Chapter 28	Detecting network and mobile incidents	626
	Introducing protocol monitoring for network	626
	Introducing protocol monitoring for mobile	

	Configuring the Protocol Monitoring condition for network detection	628
	Configuring the Protocol Monitoring condition for mobile	
	detection	
	Best practices for using network protocol matching	
	Use separate policies for specific protocols  Consider detection server network placement to support IP	630
	address matching	630
Chapter 29	Detecting endpoint events	632
	Introducing endpoint event detection	632
	About endpoint protocol monitoring	632
	About endpoint destination monitoring	633
	About endpoint application monitoring	634
	About endpoint location detection	634
	About endpoint device detection	634
	Configuring endpoint event detection conditions	635
	Configuring the Endpoint Monitoring condition	635
	Configuring the Endpoint Location condition	637
	Configuring the Endpoint Device Class or ID condition	638
	Manage and add endpoint devices	639
	Gathering endpoint device IDs	640
	Creating and modifying endpoint device configurations	
	Best practices for using endpoint detection	642
Chapter 30	Detecting described identities	643
	Introducing described identity matching	
	Described identity matching examples	
	Configuring described identity matching policy conditions	
	About Reusable Sender/Recipient Patterns	
	Configuring the Sender/User Matches Pattern condition	
	Configuring a Reusable Sender Pattern	
	Configuring the Recipient Matches Pattern condition	
	Configuring a Reusable Recipient Pattern	
	Best practices for using described identity matching	
	Define precise identity patterns to match users	
	Specify email addresses exactly to improve accuracy	
	IVIAION COMPAINS INSTEAD OF IP ACCURAGE TO IMPROVE ACCURACY	กรา

Chapter 31	Detecting synchronized identities	653
	Introducing synchronized Directory Group Matching (DGM)	
	Configuring User Groups	654
	Configuring synchronized DGM policy conditions	656
	Configuring the Sender/User based on a Directory Server Group condition	657
	Configuring the Recipient based on a Directory Server Group	
	condition  Best practices for using synchronized DGM	
	Refresh the directory on initial save of the User Group	
	Distinguish synchronized DGM from other types endpoint	059
	detection	659
Chapter 32	Detecting profiled identities	661
	Introducing profiled Directory Group Matching (DGM)	661
	About two-tier detection for profiled DGM	
	Configuring Exact Data profiles for DGM	
	Configuring profiled DGM policy conditions	
	Configuring the Sender/User based on a Profiled Directory condition	
	Configuring the Recipient based on a Profiled Directory	
	condition	
	Best practices for using profiled DGM Follow EDM best practices when implementing profiled	665
	DGM	665
	Include an email address field in the Exact Data Profile for profiled  DGM	665
	Use profiled DGM for Network Prevent for Web identity	
	detection	666
Chapter 33	Supported file formats for detection	667
	Overview of detection file format support	
	Supported formats for file type identification	
	Supported formats for content extraction	
	Supported word-processing formats for content extraction	
	Supported presentation formats for content extraction	
	Supported spreadsheet formats for content extraction	
	Supported text and markup formats for content extraction	
	Supported email formats for content extraction	
	Supported CAD formats for content extraction	690

	Supported graphics formats for content extraction	690
	Supported database formats for content extraction	690
	Other file formats supported for content extraction	691
	Supported encapsulation formats for subfile extraction	691
	Supported file formats for metadata extraction	692
	About document metadata detection	693
	Enabling server metadata detection	694
	Enabling endpoint metadata detection	694
	Best practices for using metadata detection	694
Chapter 34	Library of system data identifiers	700
	Libary of system data identifiers	701
	ABA Routing Number data identifier	702
	ABA Routing Number wide breadth	704
	ABA Routing Number medium breadth	705
	ABA Routing Number narrow breadth	705
	ABA Routing Number wide breadth	704
	ABA Routing Number medium breadth	705
	ABA Routing Number narrow breadth	705
	Australian Medicare Number data identifier	706
	Australian Tax File Number data identifier	707
	Burgerservicenummer data identifier	707
	Canadian Social Insurance Number data identifier	708
	Canadian Social Insurance Number wide breadth	710
	Canadian Social Insurance Number medium breadth	711
	Canadian Social Insurance Number narrow breadth	711
	Canadian Social Insurance Number wide breadth	710
	Canadian Social Insurance Number medium breadth	711
	Canadian Social Insurance Number narrow breadth	711
	Codice Fiscale data identifier	712
	Credit Card Magnetic Stripe Data data identifier	713
	Credit Card Number data identifier	715
	Credit Card Number wide breadth	720
	Credit Card Number medium breadth	721
	Credit Card Number narrow breadth	723
	Credit Card Number wide breadth	720
	Credit Card Number medium breadth	721
	Credit Card Number narrow breadth	723
	CUSIP Number data identifier	726
	CUSIP Number wide breadth	728
	CUSIP Number medium breadth	728
	CUSIP Number parrow breadth	729

CUSIP Number wide breadth	728
CUSIP Number medium breadth	728
CUSIP Number narrow breadth	729
Drivers License Number – CA State data identifier	730
Drivers License Number – CA State wide breadth	731
Drivers License Number – CA State medium breadth	731
Drivers License Number – CA State wide breadth	731
Drivers License Number – CA State medium breadth	731
Drivers License Number - FL, MI, MN States data identifier	732
Drivers License Number- FL, MI, MN States wide breadth	734
Drivers License Number- FL, MI, MN States medium	
breadth	
Drivers License Number- FL, MI, MN States wide breadth	734
Drivers License Number- FL, MI, MN States medium	
breadth	
Drivers License Number - IL State data identifier	
Drivers License Number- IL State wide breadth	
Drivers License Number- IL State medium breadth	
Drivers License Number- IL State wide breadth	
Drivers License Number- IL State medium breadth	
Drivers License Number - NJ State data identifier	737
Drivers License Number- NJ State wide breadth	
Drivers License Number- NJ State medium breadth	
Drivers License Number- NJ State wide breadth	
Drivers License Number- NJ State medium breadth	
Drivers License Number - NY State data identifier	
Drivers License Number- NY State wide breadth	741
Drivers License Number - NY State medium breadth	
Drivers License Number- NY State wide breadth	
Drivers License Number - NY State medium breadth	742
French INSEE Code data identifier	
Hong Kong ID data identifier	
IBAN Central data identifier	
IBAN East data identifier	745
IBAN West data identifier	748
IP Address data identifier	750
IP Address wide breadth	752
IP Address medium breadth	753
IP Address narrow breadth	754
IP Address wide breadth	
IP Address medium breadth	753
IP Address narrow breadth	
National Drug Code (NDC) data identifier	754

National Drug Code (NDC) wide breadth	756
National Drug Code (NDC) medium breadth	757
National Drug Code (NDC) narrow breadth	758
National Drug Code (NDC) wide breadth	
National Drug Code (NDC) medium breadth	757
National Drug Code (NDC) narrow breadth	758
People's Republic of China ID data identifier	
Randomized US Social Security Number (SSN) data identifier	
Singapore NRIC data identifier	
South Korea Resident Registration Number data identifier	
South Korea Resident Registration Number wide breadth	
South Korea Resident Registration Number medium breadth	
South Korea Resident Registration Number wide breadth	
South Korea Resident Registration Number medium breadth	
Spanish DNI ID data identifier	
SWIFT Code data identifier	
SWIFT Code wide breadth	
SWIFT Code narrow breadth	
SWIFT Code wide breadth	
SWIFT Code narrow breadth	
Swiss AHV Number data identifier	
Taiwan ID data identifier	
UK Drivers License Number data identifier	
UK Drivers License Number wide breadth	
UK Drivers License Number medium breadth	
UK Drivers License Number narrow breadth	
UK Drivers License Number wide breadth	
UK Drivers License Number medium breadth	
UK Drivers License Number narrow breadth	
UK Electoral Roll Number data identifier	
UK National Health Service (NHS) Number data identifier	
UK National Health Service (NHS) Number medium breadth	
UK National Health Service (NHS) Number narrow breadth	
UK National Health Service (NHS) Number medium breadth	
UK National Health Service (NHS) Number narrow breadth	
UK National Insurance Number data identifier	
UK National Insurance Number wide breadth	
UK National Insurance Number medium breadth	
UK National Insurance Number narrow breadth	
UK National Insurance Number wide breadth	
UK National Insurance Number medium breadth	
UK National Insurance Number narrow breadth	
UK Passport Number data identifier	781

	UK Passport Number wide breadth	783
	UK Passport Number medium breadth	783
	UK Passport Number narrow breadth	784
	UK Passport Number wide breadth	783
	UK Passport Number medium breadth	783
	UK Passport Number narrow breadth	784
	UK Tax ID Number data identifier	785
	UK Tax ID Number wide breadth	787
	UK Tax ID Number medium breadth	787
	UK Tax ID Number narrow breadth	787
	UK Tax ID Number wide breadth	
	UK Tax ID Number medium breadth	787
	UK Tax ID Number narrow breadth	
	US Individual Tax Identification Number (ITIN) data identifier	788
	US Individual Tax Identification Number (ITIN) wide breadth	791
	US Individual Tax Identification Number (ITIN) medium	
	breadth	791
	US Individual Tax Identification Number (ITIN) narrow	
	breadth	
	US Individual Tax Identification Number (ITIN) wide breadth	791
	US Individual Tax Identification Number (ITIN) medium	
	breadth	791
	US Individual Tax Identification Number (ITIN) narrow	
	breadth	
	US Social Security Number (SSN) data identifier	
	US Social Security Number (SSN) wide breadth	
	US Social Security Number (SSN) medium breadth	
	US Social Security Number (SSN) narrow breadth	
	US Social Security Number (SSN) wide breadth	
	US Social Security Number (SSN) medium breadth	797
	US Social Security Number (SSN) narrow breadth	798
Chapter 35	Library of policy templates	800
	Caldicott Report policy template	802
	Canadian Social Insurance Numbers policy template	804
	CAN-SPAM Act policy template	805
	Common Spyware Upload Sites policy template	806
	Competitor Communications policy template	
	Confidential Documents policy template	
	Credit Card Numbers policy template	
	Customer Data Protection policy template	808
	Data Protection Act 1998 (UK) policy template	810

Data Protection Directives (EU) policy template	. 811
Defense Message System (DMS) GENSER Classification policy	
template	813
Design Documents policy template	. 814
Employee Data Protection policy template	. 815
Encrypted Data policy template	. 817
Export Administration Regulations (EAR) policy template	. 817
FACTA 2003 (Red Flag Rules) policy template	. 818
Financial Information policy template	. 822
Forbidden Websites policy template	. 823
Gambling policy template	. 824
Gramm-Leach-Bliley policy template	
HIPAA and HITECH (including PHI) policy template	. 826
Human Rights Act 1998 policy template	. 830
Illegal Drugs policy template	
Individual Taxpayer Identification Numbers (ITIN) policy template	. 831
International Traffic in Arms Regulations (ITAR) policy template	. 832
Media Files policy template	
Merger and Acquisition Agreements policy template	
NASD Rule 2711 and NYSE Rules 351 and 472 policy template	
NASD Rule 3010 and NYSE Rule 342 policy template	
NERC Security Guidelines for Electric Utilities policy template	
Network Diagrams policy template	
Network Security policy template	
Offensive Language policy template	. 840
Office of Foreign Assets Control (OFAC) policy template	. 841
OMB Memo 06-16 and FIPS 199 Regulations policy template	
Password Files policy template	. 844
Payment Card Industry (PCI) Data Security Standard policy	
template	845
PIPEDA policy template	. 846
Price Information policy template	. 848
Project Data policy template	
Proprietary Media Files policy template	. 849
Publishing Documents policy template	. 850
Racist Language policy template	. 851
Restricted Files policy template	. 851
Restricted Recipients policy template	. 851
Resumes policy template	
Sarbanes-Oxley policy template	. 853
SEC Fair Disclosure Regulation policy template	. 855
Sexually Explicit Language policy template	. 857
Source Code policy template	858

	State Data Privacy policy template	859
	SWIFT Codes policy template	862
	Symantec DLP Awareness and Avoidance policy template	863
	UK Drivers License Numbers policy template	863
	UK Electoral Roll Numbers policy template	864
	UK National Health Service (NHS) Number policy template	864
	UK National Insurance Numbers policy template	864
	UK Passport Numbers policy template	865
	UK Tax ID Numbers policy template	865
	US Intelligence Control Markings (CAPCO) and DCID 1/7 policy	
	template	866
	US Social Security Numbers policy template	867
	Violence and Weapons policy template	867
	Webmail policy template	868
	Yahoo Message Board Activity policy template	869
	Yahoo and MSN Messengers on Port 80 policy template	870
Section 5	Configuring policy response rules	873
Chapter 36	Responding to policy violations	874
	About response rules	875
	About response rule actions	
	Response rules for all detection servers	876
	Response rules for endpoint detection	
	Response rules for Network and Mobile Prevent for Web	
	detection	
	Response rules for Network Protect detection	
	Response rule for the Classification Server	
	About response rule execution types	880
	About Automated Response rules	881
	About Smart Response rules	
	About response rule conditions	
	About response rule action execution priority	
	About response rule authoring privileges	
	Implementing response rules	
	Response rule best practices	887
Chapter 37	Configuring and managing response rules	889
	Manage response rules	889
	Adding a new response rule	
	Configuring response rules	

	About configuring Smart Response rules	892
	Configuring response rule conditions	892
	Configuring response rule actions	
	Modifying response rule ordering	
	About removing response rules	896
Chapter 38	Response rule conditions	897
	Configuring the Endpoint Location response condition	897
	Configuring the Endpoint Device response condition	
	Configuring the Incident Type response condition	
	Configuring the Incident Match Count response condition	
	Configuring the Protocol or Endpoint Monitoring response	
	condition	
	Configuring the Severity response condition	903
Chapter 39	Response rule actions	905
	Configuring the Add Note action	906
	Configuring the Limit Incident Data Retention action	
	Retaining data for endpoint incidents	907
	Discarding data for network incidents	
	Configuring the Log to a Syslog Server action	
	Configuring the Send Email Notification action	910
	Configuring the Server FlexResponse action	912
	Configuring the Set Attribute action	913
	Configuring the Set Status action	914
	Configuring the Classify Enterprise Vault Content response	
	action	915
	Configuring the retention categories that are available for	
	classification	917
	Configuring the Endpoint: FlexResponse action	919
	Configuring the Endpoint Discover: Quarantine File action	920
	Configuring the Endpoint Prevent: Block action	922
	Configuring the Endpoint Prevent: Notify action	924
	Configuring the Endpoint Prevent: User Cancel action	928
	Configuring the Network and Mobile Prevent for Web: Block FTP	
	Request action	931
	Configuring the Network and Mobile Prevent for Web: Block HTTP/S	
	action	
	Configuring the Network Prevent: Block SMTP Message action	
	Configuring the Network Prevent: Modify SMTP Message action	934
	Configuring the Network and Mobile Prevent for Web: Remove HTTP/S	
	Content action	035

	Configuring the Network Protect: Copy File action	
Section 6	Remediating and managing incidents	939
Chapter 40	Remediating incidents	940
	About incident remediation	940
	Remediating incidents	
	Executing Smart response rules	
	Incident remediation action commands	945
	Response action variables	946
	Monitor and Prevent incident variables	
	Mobile incident variables	
	Discover incident variables	948
Chapter 41	Remediating Network incidents	950
	Network incident list	950
	Network incident list—Actions	953
	Network incident list—Columns	955
	Network incident snapshot	
	Network incident snapshot—Heading and navigation	
	Network incident snapshot—General information	
	Network incident snapshot—Matches	
	Network incident snapshot—Attributes	
	Network summary report	961
Chapter 42	Remediating Endpoint incidents	964
	Endpoint incident lists	964
	Endpoint incident snapshot	967
	Reporting on Endpoint Prevent response rules	
	Endpoint incident destination or protocol-specific information	
	Endpoint incident summary reports	975
Chapter 43	Remediating Mobile incidents	977
	Mobile incident reports	977
	Mobile incident snapshot	978
	Mobile incident list	
	Mobile Prevent incident list—Actions	
	Mobile incident list—Columns	
	Mobile incident snapshot—Heading and navigation	983

	Mobile incident snapshot—General information	983
	Mobile incident snapshot—Matches	
	Mobile incident snapshot—Attributes	986
	Mobile summary report	986
Chapter 44	Remediating Discover incidents	988
	About reports for Network Discover	988
	About incident reports for Network Discover	
	Discover incident reports	990
	Discover incident snapshots	991
	Working around the issues with go to links in the Firefox browser	994
	Discover incident lists	995
	Network Discover incident actions	995
	Network Discover incident entries	996
	Discover summary reports	999
Chapter 45	Working with Classification incidents	1000
	Classification incident list	1000
	Classification incident snapshot	1001
Cl . 4.6	AA	
Chapter 46	Managing and reporting incidents	1004
	About Symantec Data Loss Prevention reports	
	About strategies for using reports	1007
	Setting report preferences	1008
	About incident reports	
	About dashboard reports and executive summaries	
	Viewing dashboards	
	Creating dashboard reports	
	Configuring dashboard reports	
	Choosing reports to include in a dashboard	
	About summary reports	
	Viewing summary reports	
	Creating summary reports	
	Viewing incidents	
	About custom reports and dashboards	
	Using IT Analytics to manage incidents	
	Filtering reports	
	Saving custom incident reports	
	Scheduling custom incident reports	
	Delivery schedule options for incident and system reports	
	Delivery schedule options for dashboard reports	1027

	Using the date widget to schedule reports	1029
	Editing custom dashboards and reports	
	Exporting incident reports	1029
	Exported fields for Network Monitor	1030
	Exported fields for Network Discover	1031
	Exported fields for Mobile Prevent for Web	1032
	Exported fields for Endpoint Discover	1033
	Deleting incidents	1034
	About the incident deletion process	1035
	Configuring the incident deletion job schedule	1036
	Starting and stopping incident deletion jobs	1037
	Working with the deletion jobs history	1037
	Deleting custom dashboards and reports	1038
	Common incident report features	1039
	Page navigation in incident reports	1039
	Incident report filter and summary options	1040
	Sending incident reports by email	1041
	Printing incident reports	1042
	Incident snapshot history tab	1042
	Incident snapshot attributes section	1043
	Incident snapshot correlations tab	
	Incident snapshot policy section	1043
	Incident snapshot matches section	
	Incident snapshot access information section	
	Customizing incident snapshot pages	1045
	About filters and summary options for reports	1046
	General filters for reports	1047
	Summary options for incident reports	
	Advanced filter options for reports	1056
Chapter 47	Archiving incidents	1065
	About incident archiving	
	Archiving incidents	
	Restoring archived incidents  Preventing incidents from being archived	
	Deleting archived incidents	
Cl		
Chapter 48	Working with incident data	1069
	About incident status attributes	1069
	Configuring status attributes and values	
	Configuring status groups	
	Export web archive	1073

	Export web archive—Create Archive	
	Export web archive—All Recent Events	1076
	About custom attributes	
	About using custom attributes	
	How custom attributes are populated	1078
	Configuring custom attributes	1079
	Setting the values of custom attributes manually	1080
Chapter 49	Working with user risk	1081
	About user risk	1081
	About user data sources	
	Defining custom attributes for user data	
	Bringing in user data	
	Viewing the user list	
	Viewing user details	
	Working with the user risk summary	
	Working with the dear not estimate	
Chapter 50	Implementing lookup plug-ins	1092
	About lookup plug-ins	1092
	Types of lookup plug-ins	
	About lookup parameters	
	About plug-in deployment	
	About plug-in chaining	
	About upgrading lookup plug-ins	
	Implementing and testing lookup plug-ins	
	Managing and configuring lookup plug-ins	
	Creating new lookup plug-ins	
	Selecting lookup parameters	
	Enabling lookup plug-ins	
	Chaining lookup plug-ins	
	Reloading lookup plug-ins	
	Troubleshooting lookup plug-ins	
	Configuring detailed logging for lookup plug-ins	
	Configuring advanced plug-in properties	
	Configuring the CSV Lookup Plug-In	
	Requirements for creating the CSV file	
	Specifying the CSV file path	
	Choosing the CSV file delimiter	
	Selecting the CSV file character set	
	Mapping attributes and parameter keys to CSV fields	
	CSV attribute mapping example	
	Testing and troubleshooting the CSV Lookup Plug-In	1118

	CSV Lookup Plug-In tutorial	1119
	Configuring LDAP Lookup Plug-Ins	1122
	Requirements for LDAP server connections	1123
	Mapping attributes to LDAP data	1123
	Attribute mapping examples for LDAP	1124
	Testing and troubleshooting LDAP Lookup Plug-ins	1125
	LDAP Lookup Plug-In tutorial	1125
	Configuring Script Lookup Plug-Ins	1127
	Writing scripts for Script Lookup Plug-Ins	1128
	Specifying the Script Command	
	Specifying the Arguments	1130
	Enabling the stdin and stdout options	1130
	Enabling incident protocol filtering for scripts	1131
	Enabling and encrypting script credentials	
	Chaining multiple Script Lookup Plug-Ins	
	Script Lookup Plug-In tutorial	
	Example script	1136
	Configuring migrated Custom (Legacy) Lookup Plug-Ins	
Chapter 51	Implementing Network Monitor	1141
Chapter 31	implementing Network Monitor	1141
	Implementing Network Monitor	
	About IPv6 support for Network Monitor	
	Choosing a network packet capture method	
	About packet capture software installation and configuration	
	Installing WinPcap on a Windows platform	
	Updating the Endace card driver	
	Installing and updating the Napatech network adapter and driver	
	software	
	Configuring the Network Monitor Server	
	Enabling GET processing with Network Monitor	
	Creating a policy for Network Monitor	
	Testing Network Monitor	1151
Chapter 52	Implementing Network Prevent for Email	1152
	Implementing Network Prevent for Email	1152
	About Mail Transfer Agent (MTA) integration	1154
	Configuring Network Prevent for Email Server for reflecting or	
	forwarding mode	1155

	Configuring Linux IP tables to reroute traffic from a restricted	
	port	
	Specifying one or more upstream mail transfer agents (MTAs)	
	Creating a policy for Network Prevent for Email	
	About policy violation data headers	
	Enabling policy violation data headers	
	Testing Network Prevent for Email	1164
Chapter 53	Implementing Network Prevent for Web	1165
	Implementing Network Prevent for Web	
	Licensing Network Prevent	
	Configuring Network Prevent for Web Server	
	About proxy server configuration	
	Proxy server compatibility with Network Prevent for Web	
	Configuring request and response mode services	
	Specifying one or more proxy servers	
	Enabling GET processing for Network Prevent for Web	
	Creating policies for Network Prevent for Web	
	Testing Network Prevent for Web	
	Troubleshooting information for Network Prevent for Web Server	11//
Section 8	Discovering where confidential data is	
	stored	1178
	360164	1170
Chapter 54	About Network Discover	1180
	About Network Discover	1180
	How Network Discover works	
Chapter 55	Setting up and configuring Network Discover	1184
	Setting up and configuring Network Discover	1184
	Modifying the Network Discover Server configuration	
	About Linux Network Discover Servers	
	Adding a new Network Discover target	
	Editing an existing Network Discover target	
Chapter 56	Network Discover scan target configuration	
chapter 30	options	1191
	Network Discover scan target configuration options	1191
	Configuring the required fields for Network Discover targets	

	Scheduling Network Discover scans  Providing the password authentication for Network Discover scanned	. 1194
	content	
	Encrypting passwords in configuration files	
	the scan	
	Filtering Discover targets by item size	
	Optimizing resources with Network Discover scan throttling	
	Creating an inventory of the locations of unprotected sensitive	. 1204
	data	1206
Chapter 57	Managing Network Discover target scans	. 1209
	Managing Network Discover target scans	1209
	Managing Network Discover Targets	
	About the Network Discover scan target list	
	Working with Network Discover scan targets	
	Removing Network Discover scan targets	
	Managing Network Discover scan histories	
	About Network Discover scan histories	
	Working with Network Discover scan histories	
	Deleting Network Discover scans	
	About Network Discover scan details	
	Working with Network Discover scan details	
	Managing Network Discover Servers	
	Viewing Network Discover server status	
	About Network Discover scan optimization	
	About the difference between incremental scans and differential	
	scans	
	About incremental scans	
	Scanning new or modified items with incremental scans	
	About managing incremental scans	
	Scanning new or modified items with differential scans	
	Configuring parallel scanning of Network Discover targets	. 1226
Chapter 58	Using Server FlexResponse plug-ins to remediate incidents	. 1228
	About the Server FlexResponse platform	
	incidents	
	Deploying a Server FlexResponse plug-in	. 1231

	Adding a Server FlexResponse plug-in to the plug-ins properties file	1232
	Creating a properties file to configure a Server FlexResponse	4000
	plug-in	
	Locating incidents for manual remediation	1236
	Using the action of a Server FlexResponse plug-in to remediate an	1007
	incident manually	
	Verifying the results of an incident response action	
	Troubleshooting a Server FlexResponse plug-in	1239
Chapter 59	Setting up scans of file shares	1241
	Setting up server scans of file systems	1241
	Supported file system targets	1242
	Automatically discovering servers and shares before configuring a file	
	system target	
	Working with Content Root Enumeration scans	
	Troubleshooting Content Root Enumeration scans	
	Automatically discovering open file shares	
	About automatically tracking incident remediation status	
	Troubleshooting automated incident remediation tracking Configuration options for Automated Incident Remediation	1249
	Tracking	1249
	Excluding internal DFS folders	
	Configuring scans of Microsoft Outlook Personal Folders (.pst	
	files)	
	Configuring and running scans of file systems	
	Optimizing file system target scanning	
	Configuring Network Protect for file shares	1258
Chapter 60	Setting up scans of Lotus Notes databases	1261
	Setting up server scans of Lotus Notes databases	1261
	Supported Lotus Notes targets	
	Configuring and running Lotus Notes scans	1262
	Configuring Lotus Notes DIIOP mode configuration scan options	1265
Chapter 61	Setting up scans of SQL databases	1267
	Setting up server scans of SQL databases	1267
	Supported SQL database targets	
	Configuring and running SQL database scans	
	Installing the JDBC driver for SQL database targets	
	SOL database scan configuration properties	

Chapter 62	Setting up scans of SharePoint servers	1274
	Setting up server scans of SharePoint servers	1274
	About scans of SharePoint servers	
	Supported SharePoint server targets	1277
	Access privileges for SharePoint scans	1277
	About Alternate Access Mapping Collections	1278
	Configuring and running SharePoint server scans	1278
	Installing the SharePoint solution on the Web Front Ends in a	
	farm	1281
	Setting up SharePoint scans to use Kerberos authentication	1283
	Troubleshooting SharePoint scans	1284
Chapter 63	Setting up scans of Exchange servers	1286
	Setting up server scans of 2007 repositories using the Exchange Web	
	Store connector	
	About scans of Exchange 2007 servers	
	Supported Exchange Server Web Store connector targets	
	Providing access rights to scan all mailboxes and public folders	
	Configuring Exchange 2007 server scans	
	Example configurations and use cases for Exchange 2007 scans	
	Troubleshooting Exchange 2007 scans	1295
	Setting up server scans of Exchange 2007 SP2 and 2010 repositories	4205
	using Exchange Web Services	
	About scans of Exchange 2007 SP2 and 2010 servers	
	Supported Exchange Server Web Services connector targets	
	Configuring Exchange 2007 SP2 and 2010 Server scans	1298
	Example configurations and use cases for Exchange 2007 SP2 and	4200
	2010 scans  Troubleshooting Exchange 2007 SP2 and 2010 scans	
	·	
Chapter 64	About Network Discover scanners	1305
	Setting up scanning of Microsoft Exchange Servers	1305
	How Network Discover scanners work	
	Troubleshooting scanners	
	Scanner processes	
	Scanner installation directory structure	
	Scanner configuration files	1311
	Scanner controller configuration options	1312

Chapter 65	Setting up scanning of file systems	1314
	Setting up remote scanning of file systems	
	Installing file system scanners	1316
	Starting file system scans	
	Installing file system scanners silently from the command line	
	Configuration options for file system scanners	1321
	Example configuration for scanning the C drive on a Windows	4000
	computer	
	Example configuration for scanning the /usr directory on UNIX	
	Example configuration for scanning with include filters	
	Example configuration for scanning with exclude filters	1324
	Example configuration for scanning with include and exclude filters	1324
	Example configuration for scanning with date filtering	
	Example configuration for scanning with file size filtering	
	Example configuration for scanning that skips symbolic links on UNIX	
	systems	
Chapter 66	Setting up scanning of Web servers	1327
	Setting up remote scanning of Web servers	1327
	Supported Web server (scanner) targets	
	Installing Web server scanners	
	Starting Web server scans	
	Configuration options for Web server scanners	
	Example configuration for a Web site scan with no authentication	
	Example configuration for a Web site scan with basic	
	authentication	1335
	Example configuration for a Web site scan with form-based	
	authentication	1336
	Example configuration for a Web site scan with NTLM	
	Example of URL filtering for a Web site scan	1336
	Example of date filtering for a Web site scan	1337
Chapter 67	Setting up scanning of Documentum repositories	1220
	repositories	1339
	Setting up remote scanning of Documentum repositories	
	Supported Documentum (scanner) targets	
	Installing Documentum scanners	
	Starting Documentum scans	
	Configuration options for Documentum scanners	1344

	Example configuration for scanning all documents in a Documentum repository	. 1346
Chapter 68	Setting up scanning of Livelink repositories	1348
	Setting up remote scanning of Livelink repositories	. 1348
	Supported Livelink scanner targets	
	Creating an ODBC data source for SQL Server	. 1349
	Installing Livelink scanners	. 1350
	Starting Livelink scans	
	Configuration options for Livelink scanners	
	Example configuration for scanning a Livelink database	. 1355
Chapter 69	Setting up Web Services for custom scan	
	targets	. 1356
	Setting up Web Services for custom scan targets	. 1356
	About setting up the Web Services Definition Language (WSDL)	
	Example of a Web Services Java client	. 1357
	Sample Java code for the Web Services example	. 1359
Section 9	Discovering and preventing data loss on	
	endpoints	. 1362
Chapter 70	Overview of Symantec Data Loss Prevention for	
	endpoints	. 1363
	About discovering and preventing data loss on endpoints	. 1363
	About policies for endpoints	. 1365
Chapter 71	Using Endpoint Prevent	. 1367
	How Endpoint Prevent works	. 1367
	About Endpoint Prevent monitoring	. 1368
	About removable storage monitoring	. 1369
	About endpoint network monitoring	. 1369
	About CD/DVD monitoring	
	About print/fax monitoring	
	About network share monitoring	
	About clipboard monitoring	
	About application monitoring	
	About virtual desktop support with Endpoint Prevent	
	About policy creation for Endpoint Prevent	. 13/5

	About monitoring policies with response rules for Endpoint	
	Servers	1375
	How to implement Endpoint Prevent	1378
	Setting the endpoint location	1378
	About Endpoint Prevent response rules in different locales	1380
Chapter 72	Using Endpoint Discover	1383
	How Endpoint Discover works	1383
	About Endpoint Discover scanning	
	About targeted Endpoint Discover scans	
	Preparing to set up Endpoint Discover	
	Creating a policy group for Endpoint Discover	
	Creating a policy for Endpoint Discover	
	Adding a rule for Endpoint Discover	
	Setting up and configuring Endpoint Discover	
	Creating an Endpoint Discover scan	
	Creating a new Endpoint Discover target	1390
	About Endpoint Discover target filters	
	Configuring Endpoint Discover scan timeout settings	1400
	Managing Endpoint Discover target scans	1401
	About managing Endpoint Discover scans	1401
	About remediating Endpoint Discover incidents	
	About rules results caching (RRC)	1403
	About Endpoint reports	1403
Chapter 73	Working with agent configurations	1405
	About agent configurations	1405
	About cloning agent configurations	
	Adding agent configurations	
	Configuring file filters	
	About the DLP Agent store	
	Advanced agent settings	
	Applying agent configurations to an agent group	
	Configuring the agent connection status	
	Enabling the communication channel for 12.0.x and earlier agents	
01 . 7.		
Chapter 74	Working with Agent Groups	1443
	About agent groups	
	Developing a strategy for deploying Agent Groups	1444
	Overview of the agent group deployment process	1//5

	Migrating pre-12.5 Endpoint deployments to agent groups	. 1446
	Creating and managing agent attributes	. 1446
	Creating a new agent attribute	. 1448
	Defining a search filter for creating user-defined attributes	. 1449
	Verifying attribute queries with the Attribute Query Resolver	
	tool	. 1449
	Applying a new attribute or changed attribute to agents	
	Undoing changes to agent attributes	
	Editing user-defined agent attributes	
	Viewing and managing agent groups	
	Agent group conditions	
	Creating a new agent group	
	Updating outdated agent configurations	
	Assigning configurations to deploy groups	
	Verify that group assignments are correct	
	Viewing group conflicts	
	Changing groups	. 1455
Chapter 75	Managing Symantec DLP Agents	. 1457
	About Symantec DLP Agent administration	1457
	Agent Overview screen	
	Agent events	
	About Symantec DLP Agent removal	
	About Endpoint Agent logs	
	Setting the log levels for an Endpoint Agent	
Chapter 76	Using application monitoring	1503
	About monitoring applications	1503
	Changing application monitoring settings	
	About adding applications	
	Adding an application	
	Using the GetAppInfo tool	
	About Application File Access monitoring	
	Implementing Application File Access monitoring	
Chapter 77	Working with Endpoint FlexResponse	. 1512
	About Endpoint FlexResponse	. 1512
	Deploying Endpoint FlexResponse	
	About deploying Endpoint FlexResponse plug-ins on endpoints	
	Deploying Endpoint FlexResponse plug-ins using a silent installation	
	process	. 1516

	About the Endpoint FlexResponse utility  Deploying an Endpoint FlexResponse plug-in using the Endpoint	. 1516
	FlexResponse utility	. 1518
	Enabling Endpoint FlexResponse on the Enforce Server	. 1519
	Uninstalling an Endpoint FlexResponse plug-in using the Endpoint	
	FlexResponse utility	. 1520
	Retrieving an Endpoint FlexResponse plug-in from a specific	
	endpoint	. 1520
	Retrieving a list of Endpoint FlexResponse plug-ins from an	
	endpoint	. 1521
Chapter 78	Using Endpoint tools	. 1523
	About Endpoint tools	. 1523
	Using Endpoint tools with Windows 7/8/8.1	
	Shutting down the agent and the watchdog services	. 1525
	Inspecting the database files accessed by the agent	. 1526
	Viewing extended log files	. 1527
	About the Device ID utility	
	Creating passwords with the password generation tool	
	Starting DLP Agents that run on Mac endpoints	. 1531
Section 10	Monitoring and preventing data loss on	
	mobile devices	4500
	mobile devices	. 1532
Chapter 79	Introducing Symantec Data Loss Prevention Mobile	
	Prevent for Web	. 1533
	How Mobile Prevent for Web works	1533
	About deploying Mobile Prevent for Web	
	About digital certificates for Mobile Prevent for Web	
	About the VPN server and VPN On Demand	
	About Microsoft Exchange ActiveSync and Mobile Prevent for	
	Web	. 1539
	Ignoring Microsoft Exchange ActiveSync monitoring	
	About mobile device management	. 1541
Chapter 80	Implementing Mobile Prevent for Web	. 1542
	Implementing Mobile Prevent for Web	. 1542
	Configuring the Mobile Prevent for Web Server	
	Configuring the VPN profile	. 1547

	About proxy server configuration for Mobile Prevent for Web	1510
	Specifying one or more proxy servers  Enabling GET processing for Mobile Prevent for Web  Creating policies for Mobile Prevent for Web  Configuring Mobile Prevent for Web for secure banking  Testing Mobile Prevent for Web	. 1550 . 1551 . 1551 . 1553
Section 11	Monitoring data loss from corporate emails downloaded to mobile devices	4555
		. 1555
Chapter 81	Introducing Symantec Data Loss Prevention Mobile Email Monitor	. 1556
	About Mobile Email Monitor	. 1557
Chapter 82	Implementing Symantec Data Loss Prevention Mobile Email Monitor	. 1559
	Symantec Data Loss Prevention Mobile Email Monitor set up	
	overview  Adding and configuring the Mobile Email Monitor Server About proxy server configuration Specifying one or more proxy servers Configuring the response mode service About digital certificates for Mobile Email Monitor Setting up native email clients for monitoring Creating policies for Mobile Email Monitor Testing Symantec Data Loss Prevention Mobile Email Monitor Troubleshooting Mobile Email Monitor Server	. 1560 . 1562 . 1562 . 1563 . 1564 . 1564 . 1564
Indev		1567

Section

# Getting started

- Chapter 1. Introducing Symantec Data Loss Prevention
- Chapter 2. Getting started administering Symantec Data Loss Prevention
- Chapter 3. Working with languages and locales

Chapter 1

# Introducing Symantec Data Loss Prevention

This chapter includes the following topics:

- About Symantec Data Loss Prevention
- About the Enforce platform
- About Network Monitor and Prevent
- About Network Discover
- About Network Protect
- About Mobile Prevent
- About Mobile Email Monitor
- About Endpoint Discover
- About Endpoint Prevent

# **About Symantec Data Loss Prevention**

Symantec Data Loss Prevention enables you to:

- Discover and locate confidential information on file and Web servers, in databases, on mobile devices, and on endpoints (desk and laptop systems)
- Protect confidential information through guarantine
- Monitor network traffic for transmission of confidential data
- Monitor and prevent the transmission of confidential data on mobile devices connected to a VPN

- Monitor the transmission of confidential data contained in corporate emails that are sent using Microsoft Exchange ActiveSync and downloaded to mobile devices
- Monitor the use of sensitive data on endpoints
- Prevent transmission of confidential data to outside locations
- Automatically enforce data security and encryption policies

Symantec Data Loss Prevention includes the following components:

Enforce Server

See "About the Enforce platform" on page 50.

See "About Symantec Data Loss Prevention administration" on page 55.

See "About the Enforce Server administration console" on page 56.

Network Discover

See "About Network Discover" on page 51.

Network Protect

See "About Network Protect" on page 52.

- Network Monitor
- Network Prevent
- Mobile Email Monitor

See "About Mobile Email Monitor" on page 53.

Mobile Prevent

See "About Mobile Prevent" on page 53.

Endpoint Discover

See "About Endpoint Discover" on page 54.

Endpoint Prevent

See "About Endpoint Prevent" on page 54.

The Discover, Protect, Monitor, Mobile Prevent, Mobile Email Monitor, and Prevent modules can be deployed as stand-alone products or in combination. Regardless of which stand-alone products you deploy, the Enforce Server is always provided for central management. Note that the Network Protect module requires the Network Discover module.

Associated with each product module are corresponding detection servers:

- Network Discover Server locates the exposed confidential data on a broad range of enterprise data repositories including:
  - File servers
  - Databases

- Microsoft SharePoint
- Lotus Notes
- **EMC Documentum**
- Livelink
- Microsoft Exchange
- Web servers
- Other data repositories

If you are licensed for Network Protect, this server also copies and guarantines sensitive data on file servers, as specified in your policies.

See "About Network Discover" on page 51.

- Network Monitor Server monitors the traffic on your network. See "About Network Monitor and Prevent" on page 51.
- Network Prevent for Email Server blocks emails that contain sensitive data. See "About Network Monitor and Prevent" on page 51.
- Network Prevent for Web Server blocks HTTP postings and FTP transfers that contain sensitive data.
  - See "About Network Monitor and Prevent" on page 51.
- Mobile Prevent for Web Server monitors and blocks HTTP/S and FTP transfers that contain sensitive data over mobile devices that are connected to a VPN. See "About Mobile Prevent" on page 53.
- Mobile Email Monitor Server monitors corporate emails that are sent through Microsoft Exchange ActiveSync and downloaded to mobile devices. See "About Mobile Email Monitor" on page 53.
- Endpoint Server monitors and prevents the misuse of confidential data on endpoints.

The distributed architecture of Symantec Data Loss Prevention allows organizations to:

- Perform centralized management and reporting.
- Centrally manage data security policies once and deploy immediately across the entire Symantec Data Loss Prevention suite.
- Scale data loss prevention according to the size of your organization.

# About the Enforce platform

The Symantec Data Loss Prevention Enforce Server is the central management platform that enables you to define, deploy, and enforce data loss prevention and security policies. The Enforce Server administration console provides a centralized, Web-based interface for deploying detection servers, authoring policies, remediating incidents, and managing the system.

See "About Symantec Data Loss Prevention" on page 47.

The Enforce platform provides you with the following capabilities:

- Build and deploy accurate data loss prevention policies. You can choose among various detection technologies, define rules, and specify actions to include in your data loss prevention policies. Using provided regulatory and best-practice policy templates, you can meet your regulatory compliance, data protection and acceptable-use requirements, and address specific security threats. See "About Data Loss Prevention policies" on page 283. See "Detecting data loss" on page 296.
- Automatically deploy and enforce data loss prevention policies. You can automate policy enforcement options for notification, remediation workflow, blocking, and encryption.
- Measure risk reduction and demonstrate compliance. The reporting features of the Enforce Server enables you to create actionable reports identifying risk reduction trends over time. You can also create compliance reports to address conformance with regulatory requirements.
  - See "About Symantec Data Loss Prevention reports" on page 1006. See "About incident reports" on page 1009.
- Empower rapid remediation. Based on incident severity, you can automate the entire remediation process using detailed incident reporting and workflow automation. Role-based access controls empower individual business units and departments to review and remediate those incidents that are relevant to their business or employees.

See "About incident remediation" on page 940. See "Remediating incidents" on page 943.

Safeguard employee privacy. You can use the Enforce Server to review incidents without revealing the sender identity or message content. In this way, multi-national companies can meet legal requirements on monitoring European Union employees and transferring personal data across national boundaries. See "About role-based access control" on page 84.

#### About Network Monitor and Prevent

The Symantec Data Loss Prevention network data monitoring and prevention products include:

#### Network Monitor

Network Monitor captures and analyzes traffic on your network. It detects confidential data and significant traffic metadata over the protocols that you specify. For example, SMTP, FTP, HTTP, and various IM protocols. You can configure a Network Monitor Server to monitor custom protocols and to use a variety of filters (per protocol) to filter out low-risk traffic.

#### Network Prevent for Email

Network Prevent for Email integrates with standard MTAs and hosted email services to provide in-line active SMTP email management. Policies that are deployed on in-line Network Prevent for Email Server direct the next-hop mail server to block, reroute, or tag email messages. These blocks are based on specific content and other message attributes. Communication between MTAs and Network Prevent for Email Server can be secured as necessary using TLS. Implement Network Monitor, review the incidents it captures, and refine your policies accordingly before you implement Network Prevent for Email. See the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent for Email.

#### Network Prevent for Web

For in-line active Web request management, Network Prevent for Web integrates with an HTTP, HTTPS, or FTP proxy server. This integration uses the Internet Content Adaptation Protocol (ICAP). The Network Prevent for Web Server detects confidential data in HTTP, HTTPS, or FTP content. When it does, it causes the proxy to reject requests or remove HTML content as specified by the governing policies.

#### About Network Discover

Network Discover scans networked file shares, Web content servers, databases, document repositories, and endpoint systems at high speeds to detect exposed data and documents. Network Discover enables companies to understand exactly where confidential data is exposed and helps significantly reduce the risk of data loss.

Network Discover gives organizations the following capabilities:

Pinpoint unprotected confidential data. Network Discover helps organizations accurately locate at risk data that is stored on their networks. You can then inform shared file server owners to protect the data.

- Reduce proliferation of confidential data. Network Discover helps organizations to detect the spread of sensitive information throughout the company and reduce the risk of data loss.
- Automate investigations and audits. Network Discover streamlines data security investigations and compliance audits. It accomplishes this task by enabling users to scan for confidential data automatically, as well as review access control and encryption policies.
- During incident remediation, Symantec Data Insight helps organizations solve the problem of identifying data owners and responsible parties for information due to incomplete or inaccurate metadata or tracking information. See the Symantec Data Loss Prevention Data Insight Implementation Guide.
- To provide additional flexibility in remediating Network Discover incidents, use the FlexResponse application programming interface (API), or the FlexResponse plug-ins that are available.
  - See the Symantec Data Loss Prevention FlexResponse Platform Developers Guide, or contact Symantec Professional Services for a list of plug-ins.

See "About Symantec Data Loss Prevention" on page 47.

#### About Network Protect

Network Protect reduces your risk by removing exposed confidential data, intellectual property, and classified information from open file shares on network servers or desktop computers. Note that there is no separate Network Protect server; the Network Protect product module adds protection functionality to the Network Discover Server.

Network Protect gives organizations the following capabilities:

- Quarantine exposed files. Network Protect can automatically move those files that violate policies to a quarantine area that re-creates the source file structure for easy location. Optionally, Symantec Data Loss Prevention can place a marker text file in the original location of the offending file. The marker file can explain why and where the original file was quarantined.
- Copy exposed or suspicious files. Network Protect can automatically copy those files that violate policies to a quarantine area. The quarantine area can re-create the source file structure for easy location, and leave the original file in place.
- Quarantine file restoration. Network Protect can easily restore quarantined files to their original or a new location.
- Enforce access control and encryption policies. Network Protect proactively ensures workforce compliance with existing access control and encryption policies.

See "About Symantec Data Loss Prevention" on page 47.

See "Configuring Network Protect for file shares" on page 1258.

#### **About Mobile Prevent**

Mobile Prevent monitors email, Web, and application communications from mobile devices to prevent sensitive information from leaving your organization. After the connection to the corporate network is established, all network traffic is sent to the Mobile Prevent for Web Server for analysis. In this way, you can protect your organization's sensitive information while allowing mobile device users to access sites and apps such as Facebook, Dropbox, and Twitter.

With Mobile Prevent, you can perform the following activities:

- Monitor confidential information leaving a mobile device through HTTP, HTTPS, or FTP traffic.
- Prevent confidential information from leaving a mobile device through HTTP, HTTPS, or FTP traffic.
- Remediate incidents originating from a mobile device.

Mobile Email Monitor and Mobile Prevent are both included in the Symantec Data Loss Prevention for Mobile license.

See "About mobile device management" on page 1541.

See "Implementing Mobile Prevent for Web" on page 1542.

See "About Symantec Data Loss Prevention" on page 47.

#### **About Mobile Email Monitor**

Mobile Email Monitor monitors corporate email that are sent through Microsoft Exchange ActiveSync and downloaded to the native email client on supported mobile devices.

With Mobile Email Monitor, you can perform the following activities:

- Monitor confidential information sent in corporate emails that are downloaded to mobile devices.
- Track what sensitive information was downloaded to monitored mobile devices that are subsequently lost or stolen.

Mobile Email Monitor and Mobile Prevent are both included in the Symantec Data Loss Prevention for Mobile license.

See Table 82-1 on page 1560.

See "About Symantec Data Loss Prevention" on page 47.

# About Endpoint Discover

Endpoint Discover detects sensitive data on your desktop or your laptop endpoints. It consists of at least one Endpoint Server and at least one Symantec DLP Agent that runs on an endpoint. You can have many Symantec DLP Agents connected to a single Endpoint Server. Symantec DLP Agents:

- Detect sensitive data in the endpoint file system.
- Collect data on that activity.
- Send incidents to the Endpoint Server.
- Send the data to the associated Endpoint Server for analysis, if necessary.

See "About Symantec Data Loss Prevention" on page 47.

# **About Endpoint Prevent**

Endpoint Prevent detects and prevents sensitive data from leaving from your desktop or your laptop endpoints. It consists of at least one Endpoint Server and all the Symantec DLP Agents running on the endpoint systems that are connected to it. You can have many Symantec DLP Agents connected to a single Endpoint Server. Endpoint Prevent detects on the following data transfers:

- Application monitoring
- CD/DVD
- Clipboard
- Email/SMTP
- eSATA removable drives
- **FTP**
- HTTP/HTTPS
- IM
- Network shares
- Print/Fax
- USB removable media devices

See "About Symantec Data Loss Prevention" on page 47.

Chapter 2

# Getting started administering Symantec Data Loss Prevention

This chapter includes the following topics:

- About Symantec Data Loss Prevention administration
- About the Enforce Server administration console
- Logging on and off the Enforce Server administration console
- About the administrator account
- Performing initial setup tasks
- Changing the administrator password
- Adding an administrator email account
- Editing a user profile
- Changing your password

# **About Symantec Data Loss Prevention administration**

The Symantec Data Loss Prevention system consists of one Enforce Server and one or more detection servers.

The Enforce Server stores all system configuration, policies, saved reports, and other Symantec Data Loss Prevention information and manages all activities.

System administration is performed from the Enforce Server administration console, which is accessed by a Firefox or Internet Explorer Web browser. The Enforce console is displayed after you log on.

See "About the Enforce Server administration console" on page 56.

After completing the installation steps in the Symantec Data Loss Prevention Installation Guide, you must perform initial configuration tasks to get Symantec Data Loss Prevention up and running for the first time. These are essential tasks that you must perform before the system can begin monitoring data on your network.

See "Performing initial setup tasks" on page 58.

### About the Enforce Server administration console

You administer the Symantec Data Loss Prevention system through the Enforce Server administration console.

The Administrator user can see and access all parts of the administration console. Other users can see only the parts to which their roles grant them access. The user account under which you are currently logged on appears at the top right of the screen.

When you first log on to the administration console, the default **Home** page is displayed. You and your users can change the default **Home** page using the Home page selection button.

See Table 2-1 on page 56.

To navigate through the system, select items from one of the four menu clusters (Home, Incidents, Policies, and System). To access the online Help, click Help at the top right of the screen.

Located in the upper-right portion of the administration console are the following navigation and operation icons:

Administration console navigation and operation icons Table 2-1

Icon	Description
	Select this page as your <b>Home</b> page. If the current screen cannot be selected as your <b>Home</b> page, this icon is unavailable.
R	Back to previous screen. Symantec recommends using this <b>Back</b> button rather than your browser <b>Back</b> button. Use of your browser <b>Back</b> button may lead to unpredictable behavior and is not recommended.

Icon	Description
<b>d</b>	Screen refresh. Symantec recommends using this <b>Refresh</b> button rather than your browser <b>Reload</b> or <b>Refresh</b> button. Use of your browser buttons may lead to unpredictable behavior and is not recommended.
	Print the current report. If the current screen contents cannot be sent to the printer, this icon is unavailable.
×	Email the current report to one or more recipients. If the current screen contents cannot be sent as an email, this icon is unavailable.

Table 2-1 Administration console navigation and operation icons (continued)

See "Logging on and off the Enforce Server administration console" on page 57.

# Logging on and off the Enforce Server administration console

If you are assigned more than one role, you can only log on under one role at a time. You must specify the role name and user name at logon.

#### To log on to the Enforce Server

- On the Enforce Server host, open a browser and point it to the URL for your server (as provided by the Symantec Data Loss Prevention administrator).
- On the Symantec Data Loss Prevention logon screen, enter your user name in the Username field. For the administrator role, this user name is always Administrator. Users with multiple roles should specify the role name and the user name in the format role\user (for example, ReportViewer\bsmith). If they do not, Symantec Data Loss Prevention assigns the user a role upon logon.

See "Configuring roles" on page 91.

- In the **Password** field, type the password. For the administrator at first logon, this password is the password you created during the installation.
  - For installation details, see the appropriate Symantec Data Loss Prevention Installation Guide.
- Click login.

The Enforce Server administration console appears. The administrator can access all parts of the administration console, but another user can see only those parts that are authorized for that particular role.

#### To log out of the Enforce Server

- 1 Click **logout** at the top right of the screen.
- 2 Click **OK** to confirm.

Symantec Data Loss Prevention displays a message confirming the logout was successful.

See "Editing a user profile" on page 60.

#### About the administrator account

The Symantec Data Loss Prevention system is preconfigured with a permanent administrator account. Note that the name is case sensitive and cannot be changed. You configured a password for the administrator account during installation.

Refer to the Symantec Data Loss Prevention Installation Guide for more information.

Only the administrator can see or modify the administrator account. Role options do not appear on the administrator configure screen, because the administrator always has access to every part of the system.

See "Changing the administrator password" on page 59.

See "Adding an administrator email account" on page 60.

# Performing initial setup tasks

After completing the installation steps in the Symantec Data Loss Prevention Installation Guide, you must perform initial configuration tasks to get Symantec Data Loss Prevention up and running for the first time. These are essential tasks that you must perform before the system can begin monitoring data on your network.

 Change the Administrator's password to a unique password only you know, and add an email address for the Administrator user account so you can be notified of various system events.

See "About the administrator account" on page 58.

- Add and configure your detection servers. See "Adding a detection server" on page 194. See "Server configuration—basic" on page 180.
- Add any user accounts you need in addition to those supplied by your Symantec Data Loss Prevention solution pack.
- Review the policy templates provided with your Symantec Data Loss Prevention solution pack to familiarize yourself with their content and data requirements. Revise the polices or create new ones as needed.

Add the data profiles that you plan to associate with policies. Data profiles are not always required. This step is necessary only if you are licensed for data profiles and if you intend to use them in policies.

# Changing the administrator password

During installation, you created a generic administrator password. When you log on for the first time, you should change this password to a unique, secret password.

See the Symantec Data Loss Prevention Installation Guide for more information.

Passwords are case-sensitive and they must contain at least eight characters.

Note that you can configure Symantec Data Loss Prevention to require strong passwords. Strong passwords are passwords specifically designed to be difficult to break. Password policy is configured from the System > Settings > General > Configure screen.

When your password expires, Symantec Data Loss Prevention displays the Password Renewal window at the next logon. When the Password Renewal window appears, type your old password, and then type your new password and confirm it.

See "Configuring user accounts" on page 99.

#### To change the administrator password

- Log on as administrator.
- 2 Click **Profile** in the upper-right corner of the administration console.
- 3 On the **Edit Profile** screen:
  - Enter your new password in the **New Password** field.
  - Re-enter your new password in the **Re-enter New Password** field. The two new passwords must be identical.

Note that passwords are case-sensitive.

Click Save.

See "About the administrator account" on page 58.

See "About the Enforce Server administration console" on page 56.

See "About the System Overview screen" on page 198.

# Adding an administrator email account

You can specify an email address to receive administrator account related messages.

#### To add or change an administrator email account

- Click **Profile** in the upper-right corner of the administration console.
- 2 Type the new (or changed) administrator email address in the email Address

The email addresses must include a fully qualified domain name. For example: my name@acme.com.

3 Click Save.

See "About the administrator account" on page 58.

See "About the Enforce Server administration console" on page 56.

See "About the System Overview screen" on page 198.

# Editing a user profile

System users can use the **Profile** screen to configure their profile passwords, email addresses, and languages.

Users can also specify their report preferences at the **Profile** screen.

To display the **Profile** screen, click **Profile** at the top-right of the Enforce Server administration console.

The **Profile** screen is divided into the following sections:

- General. Use this section to change your password, specify your email address, and choose a language preference.
- Report Preferences. Use this section to specify your preferred text encoding, CSV delimiter, and XML export preferences.
- Roles. This section displays your role. Note that this section is not displayed for the administrator because the administrator is authorized to perform all roles.

#### The **General** section:

#### To change your password

- Enter your current valid password in the **Old Password** field. 1
- 2 Enter your new password in the **New Password** field.

- 3 Re-enter your new password in the **Re-enter New Password** field.
- Click Save.

The next time you log on, you must use your new password.

See "Changing your password" on page 63.

#### To specify a new personal email address

- 1 Enter your current valid password in the **Old Password** field.
- 2 In the **Email Address** field enter your personal email address.
- 3 Click Save.

Individual Symantec Data Loss Prevention users can choose which of the available languages and locales they want to use.

#### To choose a language for individual use

- On the Enforce Server administration console, click **Profile** at the top-right of the screen.
  - Your profile appears.
- 2 In the General section of the screen, enter your password in the Old Password field.
- 3 Click the option next to your language choice.
- 4 Click Save.

The Enforce Server administration console is re-displayed in the new language.

Choosing a language profile has no effect on the detection of policy violations. Detection is performed on all content that is written in any supported language regardless of the language you choose for your profile.

See "About support for character sets, languages, and locales" on page 64.

The languages available to you are determined when the product is installed and the later addition of language packs for Symantec Data Loss Prevention. The effect of choosing a different language varies as follows:

- Locale only. If the language you choose has the notice *Translations not available*, dates and numbers are displayed in formats appropriate for the language. Reports and lists are sorted in accordance with that language. But the administration console menus, labels, screens, and Help system are not translated and remain in English.
  - See "About locales" on page 69.
- Translated. The language you choose may not display the notice *Translations* not available. In this case, in addition to the number and date format, and sort

order, the administration console menus, labels, screens, and in some cases the Help system, are translated into the chosen language.

See "About Symantec Data Loss Prevention language packs" on page 68.

#### The **Report Preferences** section:

#### To select your text encoding

- 1 Enter your current valid password in the **Old Password** field.
- 2 Select a text encoding option:
  - Use browser default encoding. Check this box to specify that text files use the same encoding as your browser.
  - Pull down menu. Click on an encoding option in the pull down menu to select it.

#### Click Save.

The new text encoding is applied to CSV exported files. This encoding lets you select a text encoding that matches the encoding that is expected by CSV applications.

#### To select a CSV delimiter

- Enter your current valid password in the **Old Password** field.
- 2 Choose one of the delimiters from the pull-down menu.
- 3 Click Save.

The new delimiter is applied to the next comma-separated values (CSV) list that you export.

See "About incident reports" on page 1009.

See "Exporting incident reports" on page 1029.

#### To select XML export details

- Enter your current valid password in the **Old Password** field.
- 2 Include Incident Violations in XML Export. If this box is checked, reports exported to XML include the highlighted matches on each incident snapshot.
- Include Incident History in XML Export. If this box is checked, reports 3 exported to XML include the incident history data that is contained in the **History** tab of each incident snapshot.
- Click Save.

Your selections are applied to the next report you export to XML.

If neither box is checked, the exported XML report contains only the basic incident information.

See "About incident reports" on page 1009.

See "Exporting incident reports" on page 1029.

# **Changing your password**

When your password expires, the system requires you to specify a new one the next time you attempt to log on. If you are required to change your password, the Password Renewal window appears.

To change your password from the Password Renewal window

- Enter your old password in the Old password field of the Password Renewal window.
- Enter your new password in the **New Password** field of the **Password Renewal** window.
- Re-enter your new password in the Re-enter New Password field of the Password Renewal window.

The next time you log on, you must use your new password.

You can also change your password at any time from the **Profile** screen.

See "Editing a user profile" on page 60.

See "About the administrator account" on page 58.

See "Logging on and off the Enforce Server administration console" on page 57.

Chapter 3

# Working with languages and locales

This chapter includes the following topics:

- About support for character sets, languages, and locales
- Supported languages for detection
- Working with international characters
- About Symantec Data Loss Prevention language packs
- About locales
- Using a non-English language on the Enforce Server administration console
- Using the Language Pack Utility

# About support for character sets, languages, and locales

Symantec Data Loss Prevention fully supports international deployments by offering a large number of languages and localization options:

- Policy creation and violation detection across many languages. The supported languages can be used in keywords, data identifiers, regular expressions, exact data profiles (EDM) and document profiles (IDM). See "Supported languages for detection" on page 65.
- Operation on localized and Multilingual User Interface (MUI) versions of Windows operating systems.

International character sets. To view and work with international character sets. the system on which you are viewing the Enforce Server administration console must have the appropriate capabilities.

See "Working with international characters" on page 67.

Locale-based date and number formats, as well as sort orders for lists and reports.

See "About locales" on page 69.

■ Localized user interface (UI) and Help system. Language packs for Symantec Data Loss Prevention provide language-specific versions of the Enforce Server administration console. They may also provide language-specific versions of the online Help system.

Note: These language packs are added separately following initial product installation.

Localized product documentation.

# **Supported languages for detection**

Symantec Data Loss Prevention supports a large number of languages for detection. Policies can be defined that accurately detect and report on the violations found in content in these languages.

Table 3-1 Languages supported by Symantec Data Loss Prevention

Language	Version 10.x	Versions 11.0, 11.1.x, 11.5, 11.6	Version 12.x
Arabic	Yes	Yes	Yes
Brazilian Portuguese	Yes	Yes	Yes
Chinese (traditional)	Yes	Yes	Yes
Chinese (simplified)	Yes	Yes	Yes
Czech	Yes	Yes	Yes
Danish	Yes	Yes	Yes
Dutch	Yes	Yes	Yes
English	Yes	Yes	Yes

(continued)			
Language	Version 10.x	Versions 11.0, 11.1.x, 11.5, 11.6	Version 12.x
Finnish	Yes	Yes	Yes
French	Yes	Yes	Yes
German	Yes	Yes	Yes
Greek	Yes	Yes	Yes
Hebrew	Yes	Yes	Yes
Hungarian	Yes	Yes	Yes
Italian	Yes	Yes	Yes
Japanese	Yes	Yes	Yes
Korean	Yes	Yes	Yes
Norwegian	Yes	Yes	Yes
Polish	Yes	Yes	Yes
Portuguese	Yes	Yes	Yes
Romanian	Yes	Yes	Yes

Table 3-1 Languages supported by Symantec Data Loss Prevention (continued)

Yes

Yes

Yes

Yes\*

Yes

Yes

Yes

Yes\*

For additional information about specific languages, see the Symantec Data Loss Prevention Release Notes.

A number of capabilities are not implied by this support:

Yes

Yes

Yes

Yes\*

Russian

Spanish

Swedish

Turkish

■ Technical support provided in a non-English language. Because Symantec Data Loss Prevention supports a particular language does not imply that technical support is delivered in that language.

<sup>\*</sup>Symantec Data Loss Prevention cannot be installed on a Windows operating system that is localized for the Turkish language, and you cannot choose Turkish as an alternate locale.

- Localized administrative user interface (UI) and documentation. Support for a language does not imply that the UI or product documentation has been localized into that language. However, even without a localized UI, user-defined portions of the UI such as pop-up notification messages on the endpoint can still be localized into any language by entering the appropriate text in the UI.
- Localized content. Keywords are used in a number of areas of the product, including policy templates and data identifiers. Support for a language does not imply that these keywords have been translated into that language. Users may, however, add keywords in the new language through the Enforce Server administration console.
- New file types, protocols, applications, or encodings. Support for a language does not imply support for any new file types, protocols, applications, or encodings that may be prevalent in that language or region other than what is already supported in the product.
- Language-specific normalization. An example of normalization is to treat accented and unaccented versions of a character as the same. The product already performs a number of normalizations, including standard Unicode normalization that should cover the vast majority of cases. However, it does not mean that all potential normalizations are included.
- Region-specific normalization and validation. An example of this is the awareness the product has of the format of North American phone numbers, which allows it to treat different versions of a number as the same, and to identify invalid numbers in EDM source files. Support for a language does not imply this kind of functionality for that language or region.

Items in these excluded categories are tracked as individual product enhancements on a language- or region-specific basis. Please contact Symantec Support for additional information on language-related enhancements or plans for the languages not listed.

See "About support for character sets, languages, and locales" on page 64.

# Working with international characters

You can use a variety of languages in Symantec Data Loss Prevention, based on:

- The operating system-based character set installed on the computer from which you view the Enforce Server administration console
- The capabilities of your browser

For example, an incident report on a scan of Russian-language data would contain Cyrillic characters. To view that report, the computer and browser you use to access the Enforce Server administration console must be capable of displaying these characters. Here are some general guidelines:

- If the computer you use to access the Enforce Server administration console has an operating system localized for a particular language, you should be able to view and use a character set that supports that language.
- If the operating system of the computer you use to access the administration console is not localized for a particular language, you may need to add supplemental language support. This supplemental language support is added to the computer you use to access the administration console, not on the Enforce Server.
  - On a Windows system, you add supplemental language support using the Control Panel > Regional and Language Options > Languages (tab) -Supplemental Language Support to add fonts for some character sets.
- It may also be necessary to set your browser to accommodate the characters you want to view and enter.

Note: The Enforce Server administration console supports UTF-8 encoded data.

On a Windows system, it may also be necessary to use the Languages -Supplemental Language Support tab under Control Panel > Regional and **Language Options** to add fonts for some character sets.

See the Symantec Data Loss Prevention Release Notes for known issues regarding specific languages.

See "About support for character sets, languages, and locales" on page 64.

# About Symantec Data Loss Prevention language packs

Language packs for Symantec Data Loss Prevention localize the product for a particular language on Windows-based systems. After a language pack has been added to Symantec Data Loss Prevention, administrators can specify it as the system-wide default. If multiple language packs have been made available by the administrator for use, individual users can choose the language they want to work in.

See "Using a non-English language on the Enforce Server administration console" on page 70.

Language pack selection results in the following:

Its locale becomes available to administrators and end users in Enforce Server Configuration screen.

- Enforce Server screens, menu items, commands, and messages appear in the language.
- The Symantec Data Loss Prevention Help system may be displayed in the language.

Language packs for Symantec Data Loss Prevention are available from Symantec File Connect.

Caution: When you install a new version of Symantec Data Loss Prevention, any language packs you have installed are deleted. For a new, localized version of Symantec Data Loss Prevention, you must upgrade to a new version of the language pack.

See "About locales" on page 69.

See "About support for character sets, languages, and locales" on page 64.

#### About locales

A locale provides the following:

- Displays dates and numbers in formats appropriate for that locale.
- Sorts lists and reports based on text columns, such as "policy name" or "file owner," alphabetically according to the rules of the locale.

Locales are installed as part of a language pack.

An administrator can also configure an additional locale for use by individual users. This additional locale need only be supported by the required version of Java.

For a list of these locales, see

http://www.oracle.com/technetwork/java/javase/javase7locales-334809.html.

The locale can be specified at product installation time, as described in the Symantec Data Loss Prevention Installation Guide. It can also be configured at a later time using the Language Pack Utility.

See "Using a non-English language on the Enforce Server administration console" on page 70.

See "About support for character sets, languages, and locales" on page 64.

# Using a non-English language on the Enforce Server administration console

The use of locales and languages is specified through the Enforce Server administration console by the following roles:

- Symantec Data Loss Prevention administrator. Specifies that one of the available languages be the default system-wide language and sets the locale.
- Individual Symantec Data Loss Prevention user. Chooses which of the available locales to use.

Note: The addition of multiple language packs could slightly affect Enforce Server performance, depending on the number of languages and customizations present. This results because an additional set of indexes has to be built and maintained for each language.

Warning: Do not modify the Oracle database NLS LANGUAGE and NLS TERRITORY settings.

See "About Symantec Data Loss Prevention language packs" on page 68.

See "About locales" on page 69.

A Symantec Data Loss Prevention administrator specifies which of the available languages is the default system-wide language.

#### To choose the default language for all users

On the Enforce Server, go to **System > Settings > General** and click Configure.

The **Edit General Settings** screen is displayed.

- Scroll to the Language section of the Edit General Settings screen, and click the button next to the language you want to use as the system-wide default.
- Click Save.

Individual Symantec Data Loss Prevention users can choose which of the available languages and locales they want to use by updating their profiles.

See "Editing a user profile" on page 60.

Administrators can use the Language Pack Utility to update the available languages.

See "Using the Language Pack Utility" on page 71.

See "About support for character sets, languages, and locales" on page 64.

Note: If the Enforce Server runs on a Linux host, you must install language fonts on the host machine using the Linux Package Manager application. Language font packages begin with fonts-<language name>. For example,

fonts-japanese-0.20061016-4.el5.noarch

# Using the Language Pack Utility

To make a specific locale available for Symantec Data Loss Prevention, you add language packs through the Language Pack Utility.

You run the Language Pack Utility from the command line. Its executable, LanguagePackUtility.exe, resides in the \SymantecDLP\Protect\bin directory.

To use the Language Pack Utility, you must have Read, Write, and Execute permissions on all of the \SymantecDLP folders and subfolders.

To display help for the utility, such as the list of valid options and their flags, enter LanguagePackUtility without any flags.

Note: Running the Language Pack Utility causes the VontuManager and VontulncidentPersister services to stop for as long as 20 seconds. Any users who are logged on to the Enforce Server administration console will be logged out automatically. When finished making its updates, the utility restarts the services automatically, and users can log back on to the administration console.

Language packs for Symantec Data Loss Prevention can be obtained from Symantec File Connect.

#### To add a language pack (Windows)

- Advise other users that anyone currently using the Enforce Server administration console must save their work and log off.
- Run the Language Pack Utility with the -a flag followed by the name of the ZIP file for that language pack. Enter:

```
LanguagePackUtility -a filename
```

where *filename* is the fully qualified path and name of the language pack ZIP file.

For example, if the Japanese language pack ZIP file is stored in c: \temp, add it by entering:

```
LanguagePackUtility -a c:\temp\Symantec DLP 12.5 Japanese.zip
```

To add multiple language packs during the same session, specify multiple file names, separated by spaces, for example:

```
LanguagePackUtility -a
c:\temp\Symantec DLP 12.5 Japanese.zip
Symantec DLP 12.5 Chinese.zip
```

3 Log on to the Enforce Server administration console and confirm that the new language option is available on the Edit General Settings screen. To do this, go to System > Settings > General > Configure > Edit General Settings.

#### To add a language pack (Linux)

- Advise other users that anyone currently using the Enforce Server administration console must save their work and log off.
- 2 Open a terminal session to the Enforce Server host and switch to the DLP system account by running the following command:

```
su - DLP system account
```

Run the following command:

```
DLP home/Protect/bin/LanguagePackUtility -a <path to language
pack zip file>
```

4 Log on to the Enforce Server administration console and confirm that the new language option is available on the Edit General Settings screen. To do this, go to System > Settings > General > Configure > Edit General Settings.

# To remove a language pack

- Advise users that anyone currently using the Enforce Server administration console must save their work and log off.
- Run the Language Pack Utility with the -r flag followed by the Java locale code of the language pack you want to remove. Enter:

```
LanguagePackUtility -r locale
```

where locale is a valid Java locale code corresponding to a Symantec Data Loss Prevention language pack.

For example, to remove the French language pack enter:

```
LanguagePackUtility -r fr FR
```

To remove multiple language packs during the same session, specify multiple file names, separated by spaces.

3 Log on to the Enforce Server administration console and confirm that the language pack is no longer available on the Edit General Settings screen. To do this, go to System > Settings > General > Configure > Edit General Settings.

Removing a language pack has the following effects:

Users can no longer select the locale of the removed language pack for individual use.

Note: If the locale of the language pack is supported by the version of Java required for running Symantec Data Loss Prevention, the administrator can later specify it as an alternate locale for any users who need it.

- The locale reverts to the system-wide default configured by the administrator.
- If the removed language was the system-wide default locale, the system locale reverts to English.

# To change or add a locale

- Advise users that anyone currently using the Enforce Server administration console must save their work and log off.
- Run the Language Pack Utility using the -c flag followed by the Java locale code for the locale that you want to change or add. Enter:

```
LanguagePackUtility -c locale
```

where locale is a valid locale code recognized by Java, such as pt PT for Portuguese.

For example, to change the locale to Brazilian Portuguese enter:

```
LanguagePackUtility -c pt BR
```

Log on to the Enforce Server administration console and confirm that the new alternate locale is now available on the Edit General Settings screen. To do this, go to System > Settings > General > Configure > Edit General Settings.

If you specify a locale for which there is no language pack, "Translations not available" appears next to the locale name. This means that formatting and sort order are appropriate for the locale, but the Enforce Server administration console screens and online Help are not translated.

Note: Administrators can only make one additional locale available for users that is not based on a previously installed Symantec Data Loss Prevention language pack.

See "About support for character sets, languages, and locales" on page 64.

Section

# Managing the Enforce Server platform

- Chapter 4. Managing Enforce Server services and settings
- Chapter 5. Managing roles and users
- Chapter 6. Connecting to group directories
- Chapter 7. Managing stored credentials
- Chapter 8. Managing system events and messages
- Chapter 9. Adding a new product module

Chapter

# Managing Enforce Server services and settings

This chapter includes the following topics:

- About Data Lost Prevention services
- About starting and stopping services on Windows
- Starting and stopping services on Linux

# **About Data Lost Prevention services**

The Symantec Data Loss Prevention services may need to be stopped and started periodically. This section provides a brief description of each service and how to start and stop the services on supported platforms.

The Symantec Data Loss Prevention services for the Enforce Server are described in the following table:

**Table 4-1** Symantec Data Loss Prevention services

Service Name	Description	
Vontu Manager	Provides the centralized reporting and management services for Symantec Data Loss Prevention.	
Vontu Monitor Controller	Controls the detection servers (monitors).	
Vontu Notifier	Provides the database notifications.	
Vontu Incident Persister	Writes the incidents to the database.	
Vontu Update	Installs the Symantec Data Loss Prevention system updates.	

See "About starting and stopping services on Windows" on page 77.

# About starting and stopping services on Windows

The procedures for starting and stopping services vary according to installation configurations and between Enforce and detection servers.

- See "Starting an Enforce Server on Windows" on page 77.
- See "Stopping an Enforce Server on Windows" on page 78.
- See "Starting a Detection Server on Windows" on page 78.
- See "Stopping a Detection Server on Windows" on page 78.
- See "Starting services on single-tier Windows installations" on page 79.
- See "Stopping services on single-tier Windows installations" on page 79.

# Starting an Enforce Server on Windows

Use the following procedure to start the Symantec Data Loss Prevention services on a Windows Enforce Server.

To start the Symantec Data Loss Prevention services on a Windows Enforce Server

- On the computer that hosts the Enforce Server, navigate to **Start > All** Programs > Administrative Tools > Services to open the Windows Services menu.
- 2 Start the Symantec Data Loss Prevention services in the following order:
  - Vontu Notifier
  - Vontu Manager
  - Vontu Incident Persister
  - Vontu Monitor Controller (if applicable)
  - Vontu Update (if necessary)

Note: Start the Vontu Notifier service first before starting other services.

See "Stopping an Enforce Server on Windows" on page 78.

# Stopping an Enforce Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows Enforce Server.

To stop the Symantec Data Loss Prevention Services on a Windows Enforce Server

- On the computer that hosts the Enforce Server, navigate to **Start > All** Programs > Administrative Tools > Services to open the Windows Services menu.
- 2 From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
  - Vontu Monitor Controller (if applicable)
  - Vontu Incident Persister
  - Vontu Manager
  - Vontu Notifier
  - Vontu Update (if necessary)

See "Starting an Enforce Server on Windows" on page 77.

# Starting a Detection Server on Windows

To start the Symantec Data Loss Prevention services on a Windows detection server

- On the computer that hosts the detection server, navigate to **Start > All** Programs > Administrative Tools > Services to open the Windows Services menu.
- Start the Symantec Data Loss Prevention services, which might include the following services:
  - Vontu Monitor
  - Vontu Update

See "Stopping a Detection Server on Windows" on page 78.

# Stopping a Detection Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows detection server.

# To stop the Symantec Data Loss Prevention Services on a Windows detection server

- On the computer that hosts the detection server, navigate to **Start > All** Programs > Administrative Tools > Services to open the Windows Services menu.
- From the **Services** menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
  - Vontu Update
  - Vontu Monitor

See "Starting a Detection Server on Windows" on page 78.

# Starting services on single-tier Windows installations

Use the following procedure to start the Symantec Data Loss Prevention services on a single-tier installation on Windows.

# To start the Symantec Data Loss Prevention services on a single-tier Windows installation

- On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to Start > All Programs > Administrative Tools > Services to open the Windows Services menu.
- 2 Start the Symantec Data Loss Prevention in the following order:
  - Vontu Notifier
  - Vontu Manager
  - Vontu Incident Persister
  - Vontu Monitor Controller (if applicable)
  - Vontu Monitor
  - Vontu Update (if necessary)

**Note:** Start the Vontu Notifier service before starting other services.

See "Stopping services on single-tier Windows installations" on page 79.

# Stopping services on single-tier Windows installations

Use the following procedure to stop the Symantec Data Loss Prevention services on a single-tier installation on Windows.

# To stop the Symantec Data Loss Prevention services on a single-tier Windows installation

- On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to Start > All Programs > Administrative Tools > Services to open the Windows Services menu.
- From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
  - Vontu Monitor
  - Vontu Monitor Controller (if applicable)
  - Vontu Incident Persister
  - Vontu Manager
  - Vontu Notifier
  - Vontu Update (if necessary)

See "Starting services on single-tier Windows installations" on page 79.

# Starting and stopping services on Linux

The procedures for starting and stopping services vary according to installation configurations and between Enforce and detection servers.

- See "Starting an Enforce Server on Linux" on page 80.
- See "Stopping an Enforce Server on Linux" on page 81.
- See "Starting a detection server on Linux" on page 81.
- See "Stopping a detection server on Linux" on page 82.
- See "Starting services on single-tier Linux installations" on page 82.
- See "Stopping services on single-tier Linux installations" on page 83.

# Starting an Enforce Server on Linux

Use the following procedure to start the Symantec Data Loss Prevention services on a Linux Enforce Server.

# To start the Symantec Data Loss Prevention services on a Linux Enforce Server

- 1 On the computer that hosts the Enforce Server, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.

Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

See "Stopping an Enforce Server on Linux" on page 81.

# Stopping an Enforce Server on Linux

Use the following procedure to stop the Symantec Data Loss Prevention services on a Linux Enforce Server.

To stop the Symantec Data Loss Prevention services on a Linux Enforce Server

- 1 On the computer that hosts the Enforce Server, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuIncidentPersister.sh stop
./VontuManager.sh stop
./VontuMonitorController.sh stop
./VontuNotifier.sh stop
```

See "Starting an Enforce Server on Linux" on page 80.

# Starting a detection server on Linux

Use the following procedure to start the Symantec Data Loss Prevention services on a Linux detection server.

# To start the Symantec Data Loss Prevention services on a Linux detection server

- 1 On the computer that hosts the detection server, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.
- 3 To start the Symantec Data Loss Prevention services, enter:

```
./VontuMonitor.sh start
./VontuUpdate.sh start
```

See "Stopping a detection server on Linux" on page 82.

# Stopping a detection server on Linux

Use the following procedure to stop the Symantec Data Loss Prevention services on a Linux detection server.

To stop the Symantec Data Loss Prevention services on a Linux detection server

- On the computer that hosts the detection server, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuMonitor.sh stop
```

See "Starting a detection server on Linux" on page 81.

# Starting services on single-tier Linux installations

Use the following procedure to start the Symantec Data Loss Prevention services on a single-tier installation on Linux.

To start the Symantec Data Loss Prevention services on a single-tier Linux installation

- On the computer that hosts the Symantec Data Loss Prevention server applications, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.

Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start
./VontuMonitor.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

See "Stopping services on single-tier Linux installations" on page 83.

# Stopping services on single-tier Linux installations

Use the following procedure to stop the Symantec Data Loss Prevention services on a single-tier installation on Linux.

To stop the Symantec Data Loss Prevention services on a single-tier Linux installation

- 1 On the computer that hosts the Symantec Data Loss Prevention servers, log on as root.
- 2 Change directory to /opt/SymantecDLP/Protect/bin.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuIncidentPersister.sh stop
./VontuManager.sh stop
./VontuMonitor.sh stop
./VontuMonitorController.sh stop
./VontuNotifier.sh stop
```

See "Starting services on single-tier Linux installations" on page 82.

Chapter 5

# Managing roles and users

This chapter includes the following topics:

- About role-based access control
- About authenticating users
- About configuring roles and users
- About recommended roles for your organization
- Roles included with solution packs
- Configuring roles
- Configuring user accounts
- Configuring password enforcement settings
- Resetting the Administrator password
- Manage and add roles
- Manage and add users
- Integrating Active Directory for user authentication
- About configuring certificate authentication

# About role-based access control

Symantec Data Loss Prevention provides role-based access control to govern how users access product features and functionality. For example, a role might let users view reports, but prevent users from creating policies or deleting incidents. Or, a role might let users author policy response rules but not detection rules.

Roles determine what a user can see and do in the Enforce Server administration console. For example, the Report role is a specific role that is included in most Symantec Data Loss Prevention solution packs. Users in the Report role can view incidents and create policies, and configure Discover targets (if you are running a Discover Server). However, users in the Report role cannot create Exact Data or Document Profiles. Also, users in the Report role cannot perform system administration tasks. When a user logs on to the system in the Report role, the Manage > Data Profiles and the System > Login Management modules in the Enforce Server administration console are not visible to this user.

You can assign a user to more than one role. Membership in multiple roles allows a user to perform different kinds of work in the system. For example, you grant the information security manager user (InfoSec Manager) membership in two roles: ISR (information security first responder) and ISM (information security manager). The InfoSec Manager can log on to the system as either a first responder (ISR) or a manager (ISM), depending on the task(s) to perform. The InfoSec Manager only sees the Enforce Server components appropriate for those tasks.

You can also combine roles and policy groups to limit the policies and detection servers that a user can configure. For example, you associate a role with the European Office policy group. This role grants access to the policies that are designed only for the European office.

See "Policy deployment" on page 288.

Users who are assigned to multiple roles must specify the desired role at log on. Consider an example where you assign the user named "User01" to two roles, "Report" and "System Admin." If "User01" wanted to log on to the system to administer the system, the user would log on with the following syntax: Login:

System Admin\User01

See "Logging on and off the Enforce Server administration console" on page 57.

The Administrator user (created during installation) has access to every part of the system and therefore is not a member of any access-control role.

See "About the administrator account" on page 58.

# About authenticating users

Symantec Data Loss Prevention provides the following options for authenticating users to the Enforce Server administration console:

Enforce Server authentication mechanisms Table 5-1

Authentication mechanism	Sign-on mechanism	Description
Password authentication	Forms-based sign-on	With password authentication, the Enforce Server administration console authenticates each user by determining if the supplied user name and password combination matches an active user account in the Enforce Server configuration. An active user account is authenticated if it has been assigned a valid role.
		When using this authentication mechanism, users enter their credentials into the Enforce Server administration console's logon page and submit them over an HTTPS connection to the Tomcat container that hosts the administration console.
		With password authentication, you must configure the user name and password of each user account directly in the Enforce Server administration console. You must also ensure that each user account has at least one assigned role.
		See "Manage and add users" on page 104.
Active Directory authentication	Forms-based sign-on	With Microsoft Active Directory authentication, the Enforce Server administration console first evaluates a supplied user name to determine if the name exists in a configured Active Directory server. If the user name exists in Active Directory, the supplied password for the user is evaluated against the Active Directory password. Any password configured in the Enforce Server configuration is ignored.
		With Active Directory authentication, you must configure a user account for each Active Directory user in the Enforce Server administration console. You do not have to enter a password for an Active Directory user account. You can switch to Active Directory authentication after you have already created user accounts in the system. However, only those existing user names that match Active Directory user names remain valid after the switch.
		<b>Note:</b> The Administrator user can log in to the Enforce Server administration console using the Enforce Server system account password that you created during installation.
		See "Verifying the Active Directory connection" on page 108.

Table 5-1 Enforce Server authentication mechanisms (continued)

Authentication mechanism	Sign-on mechanism	Description
	Single sign-on from Public Key Infrastructure (PKI)	Certificate authentication enables a user to automatically log on to the Enforce Server administration console using an X.509 client certificate that is generated by your public key infrastructure (PKI). To use certificate-based single sign-on, you must first enable certificate authentication in the Enforce Server.
		See "Configuring certificate authentication for the Enforce Server administration console" on page 112.
		The client certificate must be delivered to the Enforce Server when a client's browser performs the SSL handshake with the Enforce Server administration console. For example, you might use a smart card reader and middleware with your browser to automatically present a certificate to the Enforce Server. Or, you might obtain an X.509 certificate from a certificate authority and upload the certificate to a browser that is configured to send the certificate to the Enforce Server.
		When a user accesses the Enforce Server administration console, the PKI automatically delivers the user's certificate to the Tomcat container that hosts the administration console. The Tomcat container validates the client certificate using the certificate authorities that you have configured in the Tomcat trust store.
		See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.
		The Enforce Server administration console uses the validated certificate to determine whether the certificate has been revoked.
		See "About certificate revocation checks" on page 118.
		If the certificate is valid and has not been revoked, then the Enforce Server uses the common name (CN) in the certificate to determine if that CN is mapped to an active user account with a role in the Enforce Server configuration. For each user that will access the Enforce Server administration console using certificate-based single sign-on, you must create a user account in the Enforce Server that defines the corresponding user's CN value. You must also assign one or more valid roles to the user account.
		See "Manage and add users" on page 104.

When you install the Enforce Server, the installer prompts you to select the authentication mechanism to use. Password authentication is the default mechanism used with Symantec Data Loss Prevention, and you can use password authentication even if you also use certificate authentication. If you use certificate authentication, you can optionally disable password authentication to rely on your PKI for all access to the Enforce Server administration console.

If you upgrade from an earlier version of Symantec Data Loss Prevention, you can enable certificate authentication using manual procedures.

# About configuring roles and users

When you install the Enforce Server, you create a default Administrator user that has access to all roles. If you import a solution pack to the Enforce Server, the solution pack includes several roles and users to get you started.

See "About the administrator account" on page 58.

You may want to add roles and users to the Enforce Server. When adding roles and users, consider the following guidelines:

- Understand the roles necessary for your business users and for the information security requirements and procedures of your organization. See "About recommended roles for your organization" on page 88.
- Review the roles that created when you installed a solution pack. You can likely use several of them (or modified versions of them) for users in your organization. See "Roles included with solution packs" on page 90.
- If necessary, modify the solution-pack roles and create any required new roles. See "Configuring roles" on page 91.
- Create users and assign each of them to one or more roles. See "Configuring user accounts" on page 99.
- Manage roles and users and remove those not being used. See "Manage and add roles" on page 103. See "Manage and add users" on page 104.

# About recommended roles for your organization

To determine the most useful roles for your organization, review your business processes and security requirements.

Most businesses and organizations find the following roles fundamental when they implement the Symantec Data Loss Prevention system:

# System Administrator

This role provides access to the **System** module and associated menu options in the Enforce Server administration console. Users in this role can monitor and manage the Enforce Server and detection servers(s). Users in this role can also

deploy detection servers and run Network Discover scans. However, users in this role cannot view detailed incident information or author policies. All solution packs create a "Sys Admin" role that has system administrator privileges.

## User Administrator

This role grants users the right to manage users and roles. Typically this role grants no other access or privileges. Because of the potential for misuse, it is recommended that no more than two people in the organization be assigned this role (primary and backup).

# ■ Policy Admininistrator

This role grants users the right to manage policies and response rules. Typically this role grants no other access or privileges. Because of the potential for misuse, it is recommended that no more than two people in the organization be assigned this role (primary and backup).

# Policy Author

This role provides access to the **Policies** module and associated menu options in the Enforce Server administration console. This role is suited for information security managers who track incidents and respond to risk trends. An information security manager can author new policies or modifying existing policies to prevent data loss. All solution packs create an "InfoSec Manager" (ISM) role that has policy authoring privileges.

## Incident Responder

This role provides access to the **Incidents** module and associated menu options in the Enforce Server administration console. Users in this role can track and remediates incidents. Businesses often have at least two incident responder roles that provide two levels of privileges for viewing and responding to incidents. A first-level responder may view generic incident information, but cannot access incident details (such as sender or recipient identity). In addition, a first-level responder may also perform some incident remediation, such as escalating an incident or informing the violator of corporate security policies. A second-level responder might be escalation responder who has the ability to view incident details and edit custom attributes. A third-level responder might be an investigation responder who can create response rules, author policies, and create policy groups.

All solution packs create an "InfoSec Responder" (ISR) role. This role serves as a first-level responder. You can use the ISM (InfoSec Manager) role to provide second-level responder access.

Your business probably requires variations on these roles, as well as other roles. For more ideas about these and other possible roles, see the descriptions of the roles that are imported with solution packs.

See "Roles included with solution packs" on page 90.

# Roles included with solution packs

The various solution packs offered with Symantec Data Loss Prevention create roles and users when installed. For all solution packs there is a standard set of roles and users. You may see some variation in those roles and users, depending on the solution pack you import.

The following table summarizes the Financial Services Solution Pack roles. These roles are largely the same as the roles that are found in other Symantec Data Loss Prevention solution packs.

See Table 5-2 on page 90.

Financial Services Solution Pack roles Table 5-2

Role Name	Description		
Compliance	Compliance Officer:  Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.  This comprehensive role provides users with privileges to ensure that compliance regulations are met. It also allows users to develop strategies for risk reduction at a business unit (BU) level, and view incident trends and risk scorecards.		
Exec	Users in this role can view, remediate, and delete incidents; look up attributes; and view all custom attributes.     This role provides users with access privileges to prevent data loss risk at the macro level. Users in this role can review the risk trends and performance metrics, as well as incident dashboards.		
HRM	HR Manager:  Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.  This role provides users with access privileges to respond to the security incidents that are related to employee breaches.		
Investigator	Incident Investigator:  Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.  This role provides users with access privileges to research details of incidents, including forwarding incidents to forensics. Users in this role may also investigate specific employees.		

Table 5-2 Financial Services Solution Pack roles (continued)

Role Name	Description	
ISM	<ul> <li>InfoSec Manager:</li> <li>Users in this role can view, remediate, and delete incidents. They can look up attributes, edit all custom attributes, author all policies and policy groups, and author response rules.</li> <li>This role provides users with second-level incident response privileges. Users can manage escalated incidents within information security team.</li> </ul>	
ISR	<ul> <li>InfoSec Responder:</li> <li>Users in this role can view, remediate, and delete incidents; look up attributes; and view or edit some custom attributes. They have no access to sender or recipient identity details.</li> <li>This role provides users with first-level incident response privileges. Users can view policy incidents, find broken business processes, and enlist the support of the extended remediation team to remediate incidents.</li> </ul>	
Report	Reporting and Policy Authoring:  Users in this role can view and remediate incidents, and author all policies and policy groups. They have no access to incident details.  This role provides a single role for policy authoring and data loss risk management.	
Sys Admin	System administrator:  Users in this role can administer the system and the system users, and can view incidents. They have no access to incident details.	

# **Configuring roles**

Each Symantec Data Loss Prevention user is assigned to one or more roles that define the privileges and rights that user has within the system. A user's role determines system administration privileges, policy authoring rights, incident access, and more. If a user is a member of multiple roles, the user must specify the role when logging on, for example: Login: Sys Admin/sysadmin01.

See "About role-based access control" on page 84.

See "About configuring roles and users" on page 88.

# To configure a role

- 1 Navigate to the **System > Login Management > Roles** screen.
- 2 Click Add Role.

The Configure Role screen appears, displaying the following tabs: General, Incident Access, Policy Management, and Users.

- 3 In the **General** tab:
  - Enter a unique Name for the role. The name field is case-sensitive and is limited to 30 characters. The name you enter should be short and self-describing. Use the **Description** field to annotate the role name and explain its purpose in more details. The role name and description appear in the Role List screen.
  - In the User Privileges section, you grant user privileges for the role. System privileges(s):

# User Administration (Superuser)

Select the **User Administration** option to enable users to create additional roles and users in the Enforce Server.

# Server Administration

Select the Server Administration option to enable users to perform the following functions:

- Configure detection servers.
- Create and manage Data Profiles for Exact Data Matching (EDM), Indexed Document Matching (IDM), and Vector Machine Learning (VML).
- Configure and assign incident attributes.
- Configure system settings.
- Configure response rules.
- Create policy groups.
- Configure recognition protocols.
- View system event and traffic reports.

# People privilege:

User Select the **User Reporting** option to enable users to view the user Reporting risk summary. (Risk

**Note:** The **Incident > View** privilege is automatically enabled for all Summary, incident types for users with the **User Reporting** privilege. User

Snapshot) See "About user risk" on page 1081.

In the **Incidents** section, you grant users in this role the following incident privilege(s). These settings apply to all incident reports in the system, including the Executive Summary, Incident Summary, Incident List, and Incident Snapshots.

#### View

Select the **View** option to enable users in this role to view policy violation incidents.

You can customize incident viewing access by selecting various Actions and Display Attribute options as follows:

- By default the **View** option is enabled (selected) for all types of incidents: Network Incidents, Discover Incidents, Endpoint Incidents, Mobile Incidents, and Classification Events.
- To restrict viewing access to only certain incident types, select (highlight) the type of incident you want to authorize this role to view. (Hold down the Ctrl key to make multiple selections.) If a role does not allow a user to view part of an incident report, the option is replaced with "Not Authorized" or is blank.

**Note:** If you revoke an incident-viewing privilege for a role, the system deletes any saved reports for that role that rely on the revoked privilege. For example, if you revoke (deselect) the privilege to view network incidents, the system deletes any saved network incident reports associated with the role.

#### Actions

Select among the following **Actions** to customize the actions a user can perform when an incident occurs:

#### Remediate Incidents

This privilege lets users change the status or severity of an incident, set a data owner, add a comment to the incident history, set the **Do Not Archive** and **Allow Archive** options, and execute response rule actions. In addition, if you are using the Incident Reporting and Update API, select this privilege to remediate the location and status attributes.

#### Smart Response Rules to execute

You specify which Smart Response Rules that can be executed on a per role basis. Configured Smart Response Rules are listed in the "Available" column on the left. To expose a Smart Response Rule for execution by a user of this role, select it and click the arrow to add it to the right-side column. Use the CTRL key to select multiple rules.

# Perform attribute lookup

Lets users look up incident attributes from external sources and populate their values for incident remediation.

#### Delete incidents

Lets users delete an incident.

## Archive incidents

Lets users archive an incident.

# Restore archived incidents

Lets users restore previously archived incidents.

## Export Web archive

Lets users export a report that the system compiles from a Web archive of incidents.

## ■ Export XML

Lets users export a report of incidents in XML format.

## Email incident report as CSV attachment

Lets users email as an attachment a report containing a comma-separated listing of incident details.

# Incident Reporting and Update API

Select among the following user privileges to enable access for Web Services clients that use the Incident Reporting and Update API or the deprecated Reporting API:

■ Incident Reporting

Enables Web Services clients to retrieve incident details.

Incident Update

Enables Web Services clients to update incident details. (Does not apply to clients that use the deprecated Reporting API.)

See the Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide for more information.

# Display Attributes

Select among the following **Display Attributes** to customize what attributes appear in the Incidents view for the policy violations that users of the role can view.

**Shared** attributes are common to all types of incidents:

#### Matches

The highlighted text of the message that violated the policy appears on the **Matches** tab of the Incident Snapshot screen.

## History

The incident history.

# Body

The body of the message.

## Attachments

The names of any attachments or files.

#### Sender

The message sender.

# Recipients

The message recipients.

## Subject

The subject of the message.

## Original Message

Controls whether or not the original message that caused the policy violation incident can be viewed.

**Note:** To view an attachment properly, both the "Attachment" and the "Original Message" options must be checked.

**Endpoint** attributes are specific to Endpoint incidents:

## Username

The name of the Endpoint user.

# Machine name

The name of the computer where the Endpoint Agent is installed.

**Discover** attributes are specific to Discover incidents:

# File Owner

The name of the owner of the file being scanned.

#### Location

The location of the file being scanned.

# Custom Attributes

The Custom Attributes list includes all of the custom attributes configured by your system administrator, if any.

- Select View All if you want users to be able to view all custom attribute values.
- Select Edit All if you want users to edit all custom attribute
- To restrict the users to certain custom attributes, clear the View All and Edit All check boxes and individually select the View and/or Edit check box for each custom attribute you want viewable or editable.

**Note:** If you select Edit for any custom attribute, the View check box is automatically selected (indicated by being grayed out). If you want the users in this role to be able to view all custom attribute values, select View All.

In the **Discover** section, you grant users in this role the following privileges:

# Folder Risk Reporting

This privilege lets users view Folder Risk Reports. Refer to the Symantec Data Loss Prevention Data Insight Implementation Guide.

**Note:** This privilege is only available for Symantec Data Loss Prevention Data Insight licenses.

# Content Root Enumeration

This prvilege lets users configure and run Content Root Enumeration scans. For more information about Content Root Enumeration scans, See "Working with Content Root Enumeration scans" on page 1243.

In the Incident Access tab, configure any conditions (filters) on the types of incidents that users in this role can view.

Note: You must select the View option on the General tab for settings on the Incident Access tab to have any effect.

To add an Incident Access condition:

- Click Add Condition.
- Select the type of condition and its parameters from left to right, as if writing a sentence. (Note that the first drop-down list in a condition contains the alphabetized system-provided conditions that are associated with any custom attributes.)

For example, select **Policy Group** from the first drop-down list, select **Is** Any Of from the second list, and then select **Default Policy Group** from the final listbox. These settings would limit users to viewing only those incidents that the default policy group detected.

5 In the **Policy Management** tab, select one of the following policy privileges for the role:

## Author Policies

This role privilege lets users add, edit, and delete policies within the policy groups that are selected.

It also lets users modify system data identifiers, and create custom data identifiers.

It also lets users create and modify User Groups.

This privilege does not let users create or manage Data Profiles. This activity requires Enforce Server administrator privileges.

## Discover Scan Control

Lets the users in this role create Discover targets, run scans, and view Discover Servers.

# Credential Management

Lets users create and modify the credentials that the system requires to access target systems and perform Discover scans.

# Policy Groups

Select All Policy Groups only if users in this role need access to all existing policy groups and any that will be created in the future.

Otherwise you can select individual policy groups or the **Default Policy** Group.

Note: These options do not grant the right to create, modify, or delete policy groups. Only the users whose role includes the Server Administration privilege can work with policy groups.

# Author Response Rules

Enables users in this role to create, edit, and delete response rules.

Note: Users cannot edit or author response rules for policy remediation unless you select the **Author Response Rules** option.

Note: Preventing users from authoring response rules does not prevent them from executing response rules. For example, a user with no response-rule authoring privileges can still execute smart response rules from an incident list or incident snapshot.

- In the **Users** tab, select any users to which to assign this role. If you have not yet configured any users, you can assign users to roles after you create the users.
- 7 Click **Save** to save your newly created role to the Enforce Server database.

# Configuring user accounts

User accounts are the means by which users log onto the system and perform tasks. The role that the user account belongs to limits what the user can do in the system.

## To configure a user account:

- In the Enforce Server Administration Console, select System > Login Management > DLP Users to create a new user account or to reconfigure an existing user account. Or, click **Profile** to reconfigure the user account to which you are currently logged on.
- 2 Click **Add User** to add a new user, or click the name of an existing user to modify that user's configuration.
- 3 Enter a name for a new user account in the **Name** field.
  - The user account name must be between 8 and 30 characters long, is case-sensitive, and cannot contain backslashes (\).
  - If you use certificate authentication, the Name field value does not have to match the user's Common Name (CN). However, you may choose to use the same value for both the Name and Common Name (CN) so that you can easily locate the configuration for a specific CN. The Enforce Server administration console shows only the Name field value in the list of configured users.
  - If you are using Active Directory authentication, the user account name must match the name of the Active Directory user account. Note that all Symantec Data Loss Prevention user names are case-sensitive, even though Active Directory user names are not. Active Directory users will need to enter the case-sensitive account name when logging onto the Enforce Server administration console.
    - See "Integrating Active Directory for user authentication" on page 105.

# Configure the **Authentication** section of the **Configure User** page as follows:

## Option

#### Instructions

# **Use Password** authentication

Select this option to use password authentication and allow the user to sign on using the Enforce Server administration console log on page. This option is required if the user account will be used for a Reporting API Web Service client.

If you select this option, also enter the user password in the Password and the Re-enter Password fields. The password must be at least eight characters long and is case-sensitive. For security purposes, the password is obfuscated and each character appears as an asterisk.

If you configure advanced password settings, the user must specify a strong password. In addition, the password may expire at a certain date and the user has to define a new one periodically.

See "Configuring password enforcement settings" on page 102.

You can choose password authentication even if you also use certificate authentication. If you use certificate authentication, you can optionally disable sign on from the Enforce Server administration console log on page.

See "Disabling password authentication and forms-based log on" on page 125.

Symantec Data Loss Prevention authenticates all Reporting API clients using password authentication. If you configure Symantec Data Loss Prevention to use certificate authentication, any user account that is used to access the Reporting API Web Service must have a valid password. See the Symantec Data Loss Prevention Reporting API Developers Guide.

Note: If you configure Active Directory integration with the Enforce Server, users authenticate using their Active Directory passwords. In this case the password field does not appear on the Users screen.

See "Integrating Active Directory for user authentication" on page 105.

# **Use Certificate** authentication

Select this option to use certificate authentication and allow the user to automatically single sign-on with a certificate that is generated by a separate Private Key Infrastructure (PKI). This option is available only if you have configured certificate authentication during the Symantec Data Loss Prevention installation, or you have manually configured support for certificate authentication.

See "About authenticating users" on page 85.

See "About configuring certificate authentication" on page 110.

If you select this option, you must specify the common name (CN) value for the user in the **Common Name (CN)** field. The CN value appears in the Subject field of the user's certificate, which is generated by the PKI. Common names generally use the format, first name last name identification number.

The Enforce Server uses the CN value to map the certificate to this user account. If an authenticated certificate contains the specified CN value, all other attributes of this user account, such as the default role and reporting preferences, are applied when the user logs on.

Note: You cannot specify the same Common Name (CN) value in multiple Enforce Server user accounts.

#### Option Instructions

Account Disabled Select this option to lock the user out of the Enforce Server administration console. This option disables access for the user account regardless of which authentication mechanism you use.

> For security, after a certain number of consecutive failed logon attempts, the system automatically disables the account and locks out the user. In this case the **Account Disabled** option is checked. To reinstate the user account and allow the user to log on to the system, clear this option by unchecking it.

- 5 Optionally enter an **Email Address** and select a **Language** for the user in the **General** section of the page. The **Language** selection depends on the language pack(s) you have installed.
- In the **Report Preferences** section of the **Users** screen you specify the preferences for how this user is to receive incident reports, including Text File Encoding and CSV Delimiter.
  - If the role grants the privilege for **XML Export**, you can select to include incident violations and incident history in the XML export.
- In the **Roles** section, select the roles that are available to this user to assign data and incident access privileges.
  - You must assign the user at least one role to access the Enforce Server administration console.
  - See "Configuring roles" on page 91.
- 8 Select the **Default Role** to assign to this user at log on.

The default role is applied if no specific role is requested when the user logs on.

For example, the Enforce Server administration console uses the default role if the user uses single sign-on with certificate authentication or uses the logon page.

Note: Individual users can change their default role by clicking Profile and selecting a different option from the **Default Role** menu. The new default role is applied at the next logon.

See "About authenticating users" on page 85.

Click **Save** to save the user configuration.

**Note:** Once you have saved a new user, you cannot edit the user name.

10 Manage users and roles as necessary.

See "Manage and add roles" on page 103.

See "Manage and add users" on page 104.

# Configuring password enforcement settings

At the **Systems > Settings > General** screen you can require users to use strong passwords. Strong passwords must contain at least eight characters, at least one number, and at least one uppercase letter. Strong passwords cannot have more than two repeated characters in a row. If you enable strong passwords, the effect is system-wide. Existing users without a strong password must update their profiles at next logon.

You can also require users to change their passwords at regular intervals. In this case at the end of the interval you specify, the system forces users to create a new password.

If you use Active Directory authentication, these password settings only apply to the Administrator password. All other user account passwords are derived from Active Directory.

See "Integrating Active Directory for user authentication" on page 105.

To configure advanced authentication settings

- 1 Go to System > Settings > General and click Configure.
- 2 To require strong passwords, locate the **Password Enforcement** section and select Require Strong Passwords.
  - Symantec Data Loss Prevention prompts existing users who do not have strong passwords to create one at next logon.
- To set the period for which passwords remain valid, type a number (representing the number of days) in the Password Rotation Period field.
  - To let passwords remain valid forever, type 0 (the character for zero).

# Resetting the Administrator password

Symantec Data Loss Prevention provides the AdminPasswordReset utility to reset the Administrator's password. There is no method to recover a lost password, but you can use this utility to assign a new password. You can also use this utility if certificate authentication mechanisms are disabled and you have not yet defined a password for the Administrator account.

To use the AdminPasswordReset utility, you must specify the password to the Enforce Server database. Use the following procedure to reset the password.

# To reset the Administrator password for forms-based log on

Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

Note: If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Symantec Data Loss Prevention configuration file in the steps that follow.

- Change directory to the /opt/SymantecDLP/Protect/bin (Linux) or c:\SymantecDLP\Protect\bin (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- 3 Execute the AdminPasswordReset utility using the following syntax:

AdminPasswordReset -dbpass oracle password -newpass new administrator password

Replace *oracle* password with the password to the Enforce Server database. and replace new\_administrator\_password with the password you want to set.

# Manage and add roles

The **System > Login Management > Roles** screen displays an alphabetical list of the roles that are defined for your organization.

Roles listed on this screen display the following information:

- Name The name of the role
- **Description** A brief description of the role

Assuming that you have the appropriate privileges, you can view, add, modify, or delete roles as follows:

 Add a new role, or modify an existing one. Click **Add Role** to begin adding a new role to the system. Click anywhere in a row or the **pencil** icon (far right) to modify that role See "Configuring roles" on page 91.

■ Click the **red X** icon (far right) to delete the role; a dialog box confirms the deletion.

Before editing or deleting roles, note the following guidelines:

- If you change the privileges for a role, users in that role who are currently logged on to the system are not affected. For example, if you remove the Edit privilege for a role, users currently logged on retain permission to edit custom attributes for that session. However, the next time users log on, the changes to that role take effect, and those users can no longer edit custom attributes.
- If you revoke an incident-viewing privilege for a role, the Enforce Server automatically deletes any saved reports that rely on the revoked privilege. For example, if you revoke the privilege to view network incidents, the system deletes any saved network incident reports associated with the newly restricted role.
- Before you can delete a role, you must make sure there are no users associated with the role.
- When you delete a role, you delete all shared saved reports that a user in that role saved.

See "Manage and add users" on page 104.

# Manage and add users

The System > Login Management > DLP Users screen lists all the active user accounts in the system.

For each user account listed, the following information is listed:

- **User Name** The name the user enters to log on to the Enforce Server
- Email The email address of the user
- Access The role(s) in which the user is a member

Assuming that you have the appropriate privileges, you can add, edit, or delete user accounts as follows:

- Add a new user account, or modify an existing one. Click **Add** to begin adding a new user to the system. Click anywhere in a row or the **pencil** icon (far right) to view and edit that user account.
  - See "Configuring user accounts" on page 99.

Click the **red X** icon (far right) to delete the user account; a dialog box confirms the deletion.

Note: The Administrator account is created on install and cannot be removed from the system.

Note: When you delete a user account, you also delete all private saved reports that are associated with that user.

See "Manage and add roles" on page 103.

# Integrating Active Directory for user authentication

You can configure the Enforce Server to use Microsoft Active Directory for user authentication.

After you switch to Active Directory authentication, you must still define users in the Enforce Server administration console. If the user names you enter in the Administration Console match Active Directory users, the system associates any new user accounts with Active Directory passwords. You can switch to Active Directory authentication after you have already created user accounts in the system. Only those existing user names that match Active Directory user names remain valid after the switch.

Users must use their Active Directory passwords when they log on. Note that all Symantec Data Loss Prevention user names remain case sensitive, even though Active Directory user names are not. You can switch to Active Directory authentication after already having created user names in Symantec Data Loss Prevention. However, users still have to use the case-sensitive Symantec Data Loss Prevention user name when they log on.

## To use Active Directory authentication

Verify that the Enforce Server host is time-synchronized with the Active Directory server.

**Note:** Ensure that the clock on the Active Directory host is synched to within five minutes of the clock on the Enforce Server host.

(Linux only) Make sure that the following Red Hat RPMs are installed on the Enforce Server host:

- krb5-workstation
- krb5-libs
- pam krb5
- 3 Create the krb5.ini (or krb5.conf for Linux) configuration file that gives the Enforce Server information about your Active Directory domain structure and Active Directory server addresses.
  - See "Creating the configuration file for Active Directory integration" on page 106.
- Confirm that the Enforce Server can communicate with the Active Directory server.
  - See "Verifying the Active Directory connection" on page 108.
- 5 Configure Symantec Data Loss Prevention to use Active Directory authentication.
  - See "Configuring the Enforce Server for Active Directory authentication" on page 109.

# Creating the configuration file for Active Directory integration

You must create a krb5.ini configuration file (or krb5.conf on Linux) to give Symantec Data Loss Prevention information about your Active Directory domain structure and server locations. This step is required if you have more than one Active Directory domain. However, even if your Active Directory structure includes only one domain, it is still recommended to create this file. The kinit utility uses this file to confirm that Symantec Data Loss Prevention can communicate with the Active Directory server.

Note: If you are running Symantec Data Loss Prevention on Linux, verify the Active Directory connection using the kinit utility. You must rename the krb5.ini file as krb5.conf. The kinit utility requires the file to be named krb5.conf on Linux. Symantec Data Loss Prevention assumes that you use kinit to verify the Active Directory connection, and directs you to rename the file as krb5.conf.

Symantec Data Loss Prevention provides a sample krb5.ini file that you can modify for use with your own system. The sample file is stored in SymantecDLP\Protect\config (for example, \SymantecDLP\Protect\config On Windows or /opt/Vontu/Protect/config on Linux). If you are running Symantec Data Loss Prevention on Linux, Symantec recommends renaming the file to krb5.conf. The sample file, which is divided into two sections, looks like this:

```
[libdefaults]
 default realm = TEST.LAB
[realms]
     ENG.COMPANY.COM = {
         kdc = engAD.eng.company.com
     MARK.COMPANY.COM = {
          kdc = markAD.eng.company.com
     }
     OA.COMPANY.COM = {
          kdc = qaAD.eng.company.com
   }
```

The [libdefaults] section identifies the default domain. (Note that Kerberos realms correspond to Active Directory domains.) The [realms] section defines an Active Directory server for each domain. In the previous example, the Active Directory server for ENG.COMPANY.COM is eng.h.eng.company.com.

## To create the krb5.ini or krb5.conf file

- Go to SymantecDLP\Protect\config and locate the sample krb5.ini file. For example, locate the file in \SymantecDLP\Protect\config (on Windows) or /opt/Vontu/Protect/config (on Linux).
- 2 Copy the sample krb5.ini file to the c:\windows directory (on Windows) or the /etc directory (on Linux). If you are running Symantec Data Loss Prevention on Linux, plan to verify the Active Directory connection using the kinit command-line tool. Rename the file as krb5.conf.

See "Verifying the Active Directory connection" on page 108.

- 3 Open the krb5.ini or krb5.conf file in a text editor.
- Replace the sample default realm value with the fully qualified name of your default domain. (The value for default realm must be all capital letters.) For example, modify the value to look like the following:

```
default realm = MYDOMAIN.LAB
```

- Replace the other sample domain names with the names of your actual domains. (Domain names must be all capital letters.) For example, replace ENG. COMPANY. COM With ADOMAIN. COMPANY. COM.
- Replace the sample kdc values with the host names or IP addresses of your Active Directory servers. (Be sure to follow the specified format, in which opening brackets are followed immediately by line breaks.) For example, replace engAD.eng.company.com with ADserver.eng.company.com, and so on.

- Remove any unused kdc entries from the configuration file. For example, if you have only two domains besides the default domain, delete the unused kdc entry.
- Save the file.

# Verifying the Active Directory connection

kinit is a command-line tool you can use to confirm that the Active Directory server responds to requests. It also verifies that the Enforce Server has access to the Active Directory server. For Microsoft Windows installations, the utility is installed by the Symantec Data Loss Prevention installer in the SymantecDLP\jre\bin directory. For Linux installations, the utility is part of the Red Hat Enterprise Linux distribution, and is in the following location: /usr/kerberos/bin/kinit. You can also download Java SE 6 and locate the kinit tool in \java home\jdk1.6.0\bin.

If you run the Enforce Server on Linux, use the kinit utility to test access from the Enforce Server to the Active Directory server. Rename the krb5.ini file as krb5.conf. The kinit utility requires the file to be named krb5.conf on Linux.

See "Configuring the Enforce Server for Active Directory authentication" on page 109.

# To test the connection to the Active Directory server

- On the Enforce Server host, go to the command line and navigate to the directory where kinit is located.
- 2 Issue a kinit command using a known user name and password as parameters. (Note that the password is visible in clear text when you type it on the command line.) For example, issue the following:

```
kinit kchatterjee mypwd10#
```

The first time you contact Active Directory you may receive an error that it cannot find the krb5.ini or krb5.conf file in the expected location. On Windows, the error looks similar to the following:

krb error 0 Could not load configuration file c:\winnt\krb5.ini (The system cannot find the file specified) No error.

In this case, copy the krb5.ini or krb5.conf file to the expected location and then rerun the kinit command that is previously shown.

- Depending on how the Active Directory server responds to the command, take one of the following actions:
  - If the Active Directory server indicates it has successfully created a Kerberos ticket, continue configuring Symantec Data Loss Prevention.

If you receive an error message, consult with your Active Directory administrator.

## Configuring the Enforce Server for Active Directory authentication

Perform the procedure in this section when you first set up Active Directory authentication, and any time you want to modify existing Active Directory settings. Make sure that you have completed the prerequisite steps before you enable Active Directory authentication.

See "Integrating Active Directory for user authentication" on page 105.

### To configure the Enforce Server to user Active Directory for authentication:

- 1 Make sure all users other than the Administrator are logged out of the system.
- 2 In the Enforce Server administration console, go to System > Settings > General and click Configure (at top left).
- At the **Edit General Settings** screen that appears, locate the Active Directory Authentication section near the bottom and select (check) Perform Active **Directory Authentication.**

The system then displays several fields to fill out.

- In the **Default Active Directory Domain** field, enter the name of the default domain on your Active Directory system. This field is required. All Windows domain names must be uppercase (for example, TEST.LAB). If your setup includes a krb5.ini or krb5.conf file, the default Active Directory domain is the same as the value for default realm in the krb5.ini or krb5.conf file.
- 5 In the **Default Active Directory KDC** field, type the IP address (or the hostname) of the Active Directory server. The KDC (Key Distribution Center) is an Active Directory service that runs on port 88 by default. If the KDC is running on a different port, specify the port using the following format:

```
ipaddress or hostname:port number.
```

For example, if AD is running on the host Adserver.company.com and the KDC listens on port 53, type Adserver.company.com:53.

If you created a krb5.ini or krb5.conf file, enter the absolute path to the file in the **krb5.ini File Path** field. This file is required if your environment includes more than one domain, and recommended even if it does not. For example, type C:\winnit\krb5.ini (on Windows) or

```
/opt/Vontu/Protect/config/krb5.conf (on Linux).
```

See "Creating the configuration file for Active Directory integration" on page 106.

- If your environment has more than one Active Directory domain, enter the domain names (separated by commas) in the Active Directory Domain List field. The system displays them in a drop-down list on the user logon page. Users then select the appropriate domain at logon. Do not list the default domain, as it already appears in the drop-down list by default.
- 8 Click Save.
- 9 Go to the operating system services tool and restart the Symantec Data Loss Prevention Manager service.

# About configuring certificate authentication

Certificate authentication enables a user to automatically log on to the Enforce Server administration console using a client certificate that is generated by your public key infrastructure (PKI). When a user accesses the Enforce Server administration console, the PKI automatically delivers the user's certificate to the Tomcat container that hosts the administration console. The Tomcat container validates the client certificate using the certificate authorities that you have configured in the Tomcat trust store.

The client certificate is delivered to the Enforce Server computer when a client's browser performs the SSL handshake with the Enforce Server. For example, some browsers might be configured to operate with a smart card reader to present the certificate. As an alternative, you may choose to upload the X.509 certificate to a browser and configure the browser to send the certificate to the Enforce Server.

If the certificate is valid, the Enforce Server administration console may also determine if the certificate was revoked.

See "About certificate revocation checks" on page 118.

If the certificate is valid and has not been revoked, then the Enforce Server uses the common name (CN) in the certificate to determine if that CN is mapped to an active user account with a role in the Enforce Server configuration.

Note: Some browsers cache a user's client certificate, and will automatically log the user onto the Administration Console after the user has chosen to sign out. In this case, users must close the browser window to complete the log out process.

The following table describes the steps necessary to use certificate authentication with Symantec Data Loss Prevention.

Table 5-3 Configuring certificate authentication

Phase	Action	Description
Phase 1	Enable certificate authentication on the Enforce Server computer.	You can enable certificate authentication when you install the Enforce Server, or you can reconfigure an existing Enforce Server to enable authentication.
		See "Configuring certificate authentication for the Enforce Server administration console" on page 112.
Phase 2	Add certificate authority (CA) certificates to establish the trust chain.	You can add CA certificates to the Tomcat trust store when you install the Enforce Server. Or, you can use the Java keytool utility to manually add certificates to an existing Enforce Server.
		See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.
Phase 3	(Optional) Change the Tomcat trust store password.	The Symantec Data Loss Prevention installer configures each new Enforce Server installation with a default Tomcat trust store password. Follow these instructions to configure a secure password.  See "Changing the Tomcat trust store password" on page 115.
Phase 4	Map certificate common name (CN) values to Enforce Server user accounts.	See "Mapping Common Name (CN) values to Symantec Data Loss Prevention user accounts" on page 117.
Phase 5	Configure the Enforce Server to check for certificate revocation.	See "About certificate revocation checks" on page 118.
Phase 6	Verify Enforce Server access using certificate-based single sign-on.	See "Troubleshooting certificate authentication" on page 124.

Phase	Action	Description
Phase 7	(Optional) Disable forms-based log on.	If you want to use certificate-based single sign-on for all access to the Enforce Server, disable forms-based log on.
		See "Disabling password authentication and forms-based log on" on page 125.

Table 5-3 Configuring certificate authentication (continued)

## Configuring certificate authentication for the Enforce Server administration console

If you selected certificate authentication as the single sign-on option when you installed Symantec Data Loss Prevention, then the Enforce Server administration console is already configured to support certificate authentication.

Follow this procedure to manually enable certificate authentication on an upgraded Symantec Data Loss Prevention installation, or to disable or verify certificate authentication on the Enforce Server. Or, follow this procedure if you want to disable password authentication (and forms-based log on) for the Enforce Server.

### To configure certificate authentication for the Enforce Server administration console

Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

Note: If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Symantec Data Loss Prevention configuration file in the steps that follow.

- Change directory to the /opt/SymantecDLP/Protect/config (Linux) or c:\SymantecDLP\Protect\config (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- Open the Manager.properties file with a text editor.

To enable or verify certificate authentication, add or edit the following line in the file:

```
com.vontu.manager.certificate authentication = true
```

To disable certificate authentication, change the value to "false." However, if you disable certificate authentication, also ensure that you have enabled password authentication to ensure that you can log into the Enforce Server administration console. To enable password authentication, add or edit the line:

```
com.vontu.manager.form authentication = true
```

Set this option to false (disable forms-based log on) only if you want to require a valid certificate for all Enforce Server administration console accounts, including Administrator accounts. Ensure that you have installed all necessary certificates and you have verified that users can log on using certificate authentication.

See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.

- Save your changes and exit the text editor. 5
- Change directory to the /opt/SymantecDLP/Protect/tomcat/conf (Linux) or c:\SymantecDLP\Protect\tomcat\conf (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- 7 Open the server.xml file with a text editor.
- To enable or verify certificate authentication, add or edit the option clientAuth="want" as shown in the following line in the file:

```
<Connector URIEncoding="UTF-8" acceptCount="100" clientAuth="want"</pre>
debug="0" disableUploadTimeout="true" enableLookups="false"
keystoreFile="conf/.keystore" keystorePass="protect"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
port="443" scheme="https" secure="true" sslProtocol="TLS"
truststoreFile="conf/truststore.jks" truststorePass="protect"/>
```

- **9** Save your changes and exit the text editor.
- 10 Stop and then restart the Vontu Manager service to apply your changes.
- 11 Configure and enable certificate revocation.

See "About certificate revocation checks" on page 118.

## Adding certificate authority (CA) certificates to the Tomcat trust store

This procedure is required only if you did not import CA certificates during the Symantec Data Loss Prevention installation, or if you upgraded an earlier Symantec Data Loss Prevention installation and you are configuring certificate authentication. This procedure is also required to add OCSP responder certificates to the truststore for some OCSP configurations.

To use certificate authentication with Symantec Data Loss Prevention, you must add to the Tomcat trust store all CA certificates that are required to authenticate users in your system. Each X.509 certificate must be provided in Distinguished Encoding Rules (DER) format in a .cer file. If multiple CAs are required to establish the certificate chain, then you must add multiple .cer files.

#### To add certificate CA certificates to the Tomcat trust store

Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

Note: If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Tomcat configuration files in the steps that follow.

- 2 Change directory to the /opt/SymantecDLP/Protect/tomcat/conf (Linux) or c:\SymantecDLP\Protect\tomcat\conf (Windows) directory. If you installed Symantec Data Loss Prevention to a different directory, substitute the correct path.
- 3 Copy all certificate files (.cer files) that you want to import to the conf directory on the Enforce Server computer.

4 Use the keytool utility installed with Symantec Data Loss Prevention to add a certificate to the Tomcat truststore. For Windows systems, enter:

```
c:\SymantecDLP\jre\bin\keytool -import -trustcacerts
  -alias CA CERT 1
  -file certificate 1.cer
  -keystore .\truststore.jks
                       For Linux systems, enter:
```

```
/opt/SymantecDLP/jre/bin/keytool -import -trustcacerts
   -alias CA CERT 1
  -file certificate 1.cer
   -keystore ./truststore.jks
```

In the above commands, replace CA\_CERT\_1 with a unique alias for the certificate that you are importing. Replace certificate 1.cer with the name of the certificate file you copied to the Enforce Server computer.

- Enter the password to the keystore when the keytool utility prompts you to do so. If you did not change the default keystore password, then the password is "protect."
- Repeat these steps to install all the certificate files that are necessary to complete the certificate chain.
- 7 Stop and then restart the Vontu Manager service to apply your changes.
- 8 If you have not yet changed the default Tomcat keystore password, do so now. See "Changing the Tomcat trust store password" on page 115.

## Changing the Tomcat trust store password

When you install Symantec Data Loss Prevention, the Tomcat trust store uses the default password, "protect." Follow this procedure to assign a secure password to the Tomcat trust store when using certificate authentication.

### To change the Tomcat trust store password

Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

**Note:** If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Tomcat configuration files in the steps that follow.

- Change directory to the /opt/SymantecDLP/Protect/tomcat/conf (Linux) or c:\SymantecDLP\Protect\tomcat\conf (Windows) directory. If you installed Symantec Data Loss Prevention to a different directory, substitute the correct path.
- Use the keytool utility installed with Symantec Data Loss Prevention to change the Tomcat truststore password. For Windows systems, enter:

c:\SymantecDLP\jre\bin\keytool -storepasswd -new new password -keystore ./truststore.jks

For Linux systems, enter:

/opt/SymantecDLP/jre/bin/keytool -storepasswd -new new password -keystore ./truststore.jks

In the above commands, replace *new\_password* with a secure password.

- Enter the current password to the keystore when the keytool utility prompts 4 you to do so. If you did not change the default keystore password, then the password is "protect."
- 5 Change directory to the /opt/SymantecDLP/Protect/tomcat/conf (Linux) or c:\SymantecDLP\Protect\tomcat\conf (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- Open the server.xml file with a text editor.

In the following line in the file, edit the truststorePass="protect" entry to specify your new password:

```
<Connector URIEncoding="UTF-8" acceptCount="100" clientAuth="want"</pre>
debug="0" disableUploadTimeout="true" enableLookups="false"
keystoreFile="conf/.keystore" keystorePass="protect"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
port="443" scheme="https" secure="true" sslProtocol="TLS"
truststoreFile="conf/truststore.jks" truststorePass="protect"/>
```

Replace protect with the new password that you defined in the keytool command.

- 8 Save your changes and exit the text editor.
- Change directory to the /opt/SymantecDLP/Protect/config (Linux) or c:\SymantecDLP\Protect\config (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- 10 Open the Manager.properties file with a text editor.
- **11** Add the following line in the file to specify the new password:

```
com.vontu.manager.tomcat.truststore.password = password
```

Replace password with the new password. Do not enclose the password with quotation marks.

- 12 Save your changes and exit the text editor.
- 13 Stop and then restart the Vontu Manager service to apply your changes.

## Mapping Common Name (CN) values to Symantec Data Loss Prevention user accounts

Each user that will access the Enforce Server administration console using certificate-based single sign-on must have an active user account in the Enforce Server configuration. The user account associates the common name (CN) value from the user's client certificate to one or more roles in the Enforce Server administration console. You can map a CN value to only one Enforce Server user account.

The user account that you create does not require a separate Enforce Server administration console password. However, you can optionally configure a password if you want to allow the user to also log on from the Enforce Server administration console log on page. If you enable password authentication and the user does not provide a certificate when the browser asks for one, then the Enforce Server displays the log on page. (If password authentication is disabled, a log on failure is displayed if the user does not provide a certificate.)

In order for a user to log on using single sign-on with certificate authentication, an active user account must identify the user's CN value, and it must be assigned a valid role in the Enforce Server configuration. If you want to prevent a user from accessing the Enforce Server administration console without revoking the user's client certificate, disable or delete the associated Enforce Server user account.

See "Configuring user accounts" on page 99.

## About certificate revocation checks

While managing your public key infrastructure, you will periodically need to revoke a client's certificate with the CA. For example, you might revoke a certificate if an employee leaves the company, or if an employee's credentials are lost or stolen. When you revoke a certificate, the CA uses one or more Certificate Revocation Lists (CRLs) to publish those certificates that are no longer valid. Symantec Data Loss Prevention also supports the use of an Online Certificate Status Protocol (OCSP) responder, which clients can use to determine if a particular certificate has been revoked. The OCSP responder can be implemented as a service on your CA server, or as a separate OCSP server.

OCSP is the first mechanism that Symantec Data Loss Prevention uses to perform certificate revocation checks. After the Tomcat container has determined that a client certificate is valid, the Enforce Server sends an OCSP request to a designated OCSP responder to determine if the certificate was revoked. The information used to contact the OCSP responder can be provided in one of two ways:

 The Authority Information Access (AIA) field in a client certificate. The client certificate itself can include the URL of the OCSP responder in an AIA field. The following shows an example AIA field that defines an OCSP responder:

```
[1] Authority Info Access Access Method=On-line
Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name: URL=http://my ocsp responder
```

This method is commonly used when you configure an internal CA to provide the OCSP responder service. If the OCSP responder specified in the AIA field is directly accessible from the Enforce Server computer, then no additional configuration is required to perform revocation checks. However, if the OCSP responder is accessible only by a proxy server, then you must configure the proxy server settings in the Symantec Data Loss Prevention configuration.

The OCSP configuration file. As an alternative, you can manually configure OCSP responder properties using the manager-certauth.security configuration file. If you choose to use this file, the configuration in the file

overrides any information that is present in a client certificate's AIA field. This method is commonly used if you want to use a local OCSP responder instead of the one specified in the AIA field, or if your client certificates do not include an AIA field.

See "Manually configuring OCSP responder properties" on page 123.

Note: If the OCSP responder that you configure in this file does not use the CA certificate to sign its responses, then you must add the OCSP responder's certificate to the Tomcat trust store.

See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.

If a certificate's revocation status cannot be determined using OCSP, then Symantec Data Loss Prevention retrieves revocation lists from a Certificate Revocation List Distribution Point (CRLDP). To check revocation using a CRLDP, the client certificate must include a CRL distribution point field. The following shows an example CRLDP field definition:

```
[1]CRL Distribution Point
 Distribution Point Name:
   Full Name: URL=http://my crldp
```

Note: Symantec Data Loss Prevention does not support specifying the CRLDP using an LDAP URL.

If the CRL distribution point is defined in each certificate and the Enforce Server can directly access the server, then no additional configuration is required to perform revocation checks. However, if the CRL distribution point is accessible only by a proxy server, then you must configure the proxy server settings in the Symantec Data Loss Prevention configuration.

See "Accessing the OCSP responder or CRLDP with a proxy" on page 121.

Regardless of which revocation checking method you use, you must enable certificate revocation checks on the Enforce Server computer. Certificate revocation checks are enabled by default if you select certificate installation during the Enforce Server installation. If you upgraded an existing Symantec Data Loss Prevention installation, certificate revocation is not enabled by default.

See "Configuring certificate revocation checks" on page 120.

If the Enforce Server computer must use a proxy to access either the OCSP responder service or CRLDP, then you must configure the proxy settings on the Enforce Server computer.

See "Accessing the OCSP responder or CRLDP with a proxy" on page 121.

If you are using OCSP for revocation checks but certificate client certificate AIA fields do not specify a valid OCSP responder, then you must manually configure OCSP responder properties in the manager-certauth.security configuration file.

See "Manually configuring OCSP responder properties" on page 123.

### Configuring certificate revocation checks

When you enable certificate revocation checks, Symantec Data Loss Prevention uses OCSP to determine if each client certificate was revoked by a certificate authority. If the certificate status cannot be determined using OCSP, Symantec Data Loss Prevention uses a CRLDP to determine the revocation status.

Follow this procedure to enable certificate revocation checks.

### To configure certificate revocation checks

- Ensure that the OCSP responder is configured, either in the AIA field of each certificate or in the manager-certauth.security file.
  - See "About certificate revocation checks" on page 118.
  - See "Manually configuring OCSP responder properties" on page 123.
- 2 Ensure that the CRLDP is defined in the CRL distribution point field of each client certificate.
- Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

Note: If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Symantec Data Loss Prevention configuration file in the steps that follow.

- Change directory to the /opt/SymantecDLP/Protect/config (Linux) or c:\SymantecDLP\Protect\config (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- 5 Open the VontuManager.conf file with a text editor.

6 To enable certificate revocation checks, add or edit the following line in the file:

wrapper.java.additional.18 = - Dcom.sun.net.ssl.checkRevocation = true

To disable the checks, change the value to "false."

If you want to configure the OCSP responder server manually, rather than using the AIA field in client certificates, edit the following line in the file:

wrapper.java.additional.19 -- Djava.security.properties - . . / config/manager-certauth.security

Also enable this line in the file if you want to disable OCSP revocation checking. (You can then configure a property in manager-certauth.security to disable OCSP checks.)

Ensure that the configuration parameter points to the indicated OCSP configuration file. Always edit the existing manager-certauth.security file, rather than creating a new file.

See "Manually configuring OCSP responder properties" on page 123.

To enable revocation checking using a CRLDP, add or uncomment the following line in the file:

```
wrapper.java.additional.21=-Dcom.sun.security.enableCRLDP=true
```

This option is enabled by default for new Symantec Data Loss Prevention installations.

If you are using CRLDP revocation checks, optionally configure the cache lifetime using the property:

wrapper.java.additional.20 =- Dsun.security.certpath.ldap.cache.lifetime=30

This parameter specifies the length of time, in seconds, to cache the revocation lists that are obtained from a CRL distribution point. After this time is reached, a lookup is performed to refresh the cache the next time there is an authentication request. 30 seconds is the default cache lifetime. Specify 0 to disable the cache, or -1 to store cache results indefinitely.

10 Stop and then restart the Vontu Manager service to apply your changes.

## Accessing the OCSP responder or CRLDP with a proxy

Symantec recommends that you allow direct access from the Enforce Server computer to all OCSP responder servers and CRLDP servers that are required to perform certificate revocation checks. However, if the OCSP responder or the CRLDP server are accessible only through a proxy, then you must configure the proxy settings on the Enforce Server computer.

When you configure a proxy, the Enforce Server uses your proxy configuration for all HTTP connections, such as those connections that are created when connecting to a Data Insight server to fetch certificates. Check with your proxy administrator before you configure these proxy settings, and consider allowing direct access to OCSP and CRDLP servers if at all possible.

### To configure proxy settings for an OCSP responder or CRLDP server

- Ensure that the OCSP responder is configured in the AIA field of each certificate.
  - See "About certificate revocation checks" on page 118.
- Ensure that the CRLDP is defined in the CRL distribution point field of each client certificate.
- 3 Log onto the Enforce Server computer using the account that you created during Symantec Data Loss Prevention installation.

Note: If you log on with a different account (such as the root or Administrator account) ensure that you do not change the permissions or ownership on any Symantec Data Loss Prevention configuration file in the steps that follow.

- 4 Change directory to the /opt/SymantecDLP/Protect/config (Linux) or c:\SymantecDLP\Protect\config (Windows) directory. If you installed Symantec Data Loss Prevention into a different directory, substitute the correct path.
- 5 Open the VontuManager.conf file with a text editor.
- Add or edit the following configuration properties to identify the proxy:

```
wrapper.java.additional.22 = - Dhttp.proxyHost = myproxy.mydomain.com
wrapper.java.additional.23=-Dhttp.proxyPort=8080
wrapper.java.additional.24=-Dhttp.nonProxyHosts=hosts
```

Replace myproxy.mydomain.com and 8080 with the host name and port of your proxy server. Replace hosts with one or more accessible OCSP responder to use if the proxy is unavailable. You can include server host names, fully qualified domain names, or IP addresses separated with a pipe character. For example:

```
wrapper.java.additional.24=-Dhttp.nonProxyHosts=ocsp-server|
127.0.0.1|DataInsight Server Host
```

- 7 Save your changes to the configuration file.
- 8 Stop and then restart the Vontu Manager service to apply your changes.

## Manually configuring OCSP responder properties

You can optionally edit the manager-certauth.security file to configure OCSP connection parameters for your system. By default, this file enables OCSP checks, but all other options are commented and inactive. If you uncomment any parameters in the file, those parameters override the OCSP configuration that is present in the AIA fields of a client certificate.

See "About certificate revocation checks" on page 118.

Note: If the OCSP responder that you configure in this file does not use the CA certificate to sign its responses, then you must add the OCSP responder's certificate to the Tomcat trust store.

See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.

manager-certauth.security is located in the /opt/SymantecDLP/Protect/config (Linux) or c:\SymantecDLP\Protect\config (Windows) directory. Always edit the existing manager-certauth.security file, rather than create a new file. You may want to backup the file before making your changes to preserve the original contents. The manager-certauth.security contains additional information about these parameters

The file contains the following parameters.

Table 5-4 OCSP configuration parameters

Configuration parameter with example	Description
ocsp.enable=true	This parameter enables OCSP for revocation checks if certificate revocation is also enabled in the VontuManager.properties file. This parameter is enabled by default for all Symantec Data Loss Prevention installations. Disable the property if you want to use only CRLDP checks instead of OCSP.
ocsp.responderURL=http://ocsp.example.net:80	Defines the URL of OCSP responder. If you do not define this parameter, the URL is taken from the AIA field in the client certificate, if available.

Table 5-4 OCSP configuration parameters (continued)

Configuration parameter with example	Description
ocsp.responderCertSubjectName=CN=OCSP Responder, O=XYZ Corp	Defines the subject name of the certificate that corresponds to the OCSP responder. By default Symantec Data Loss Prevention assumes that the certificate of the issuer of the client certificate corresponds to the OCSP responder's certificate. If you do not use this default configuration, you must identify the OCSP responder's certificate in some other way. You must also add the OCSP responder certificate to the Tomcat trust store.
	See "Adding certificate authority (CA) certificates to the Tomcat trust store" on page 114.
	If you cannot accurately identify the certificate of the OCSP responder using only the subject name, then use both the ocsp.responderCertIssuerName and ocsp.responderCertSerialNumber parameters instead of ocsp.responderCertSubjectName. (If you define ocsp.responderCertSubjectName, then the remaining two parameters in this table are ignored.)
ocsp.responderCertIssuerName=CN=Enterprise CA, O=XYZ Corp	Use this parameter in combination with ocsp.responderCertSerialNumber to identify the OCSP responder certificate. This parameter defines the certificate issuer of the OCSP responder's certificate.  If you use this parameter, do not also use the ocsp.responderCertSubjectName parameter.
ocsp.responderCertSerialNumber=2A:FF:00	Use this parameter in combination with ocsp.responderCertIssuerName to identify the OCSP responder certificate. This parameter defines the serial number of the OCSP responder's certificate.
	If you use this parameter, do not also use the ocsp.responderCertSubjectName parameter.

## Troubleshooting certificate authentication

By default Symantec Data Loss Prevention logs each successful log on request to the Enforce Server administration console. Symantec Data Loss Prevention also logs an error message if a logon request is made without supplying a certificate, or if a valid certificate presents a CN that does not map to a valid user account in the Enforce Server configuration.

Note: If certificate authentication fails while the browser is establishing an HTTPS connection to the Enforce Server administration console, then Symantec Data Loss Prevention cannot log an error message.

You can optionally log additional information about certificate revocation checks by adding or uncommenting the following system property in the VontuManager.conf file:

```
wrapper.java.additional.90=-Djava.security.debug=certpath
```

VontuManager.conf is located in the c:\SymantecDLP\Protect\config (Windows) or /opt/SymantecDLP/Protect/config (Linux) directory. All debug messages are logged to c:\SymantecDLP\Protect\logs\debug\VontuManager.log (Windows) Of /var/log/SymantecDLP/debug/VontuManager.log (Linux).

## Disabling password authentication and forms-based log on

Forms-based log on with password authentication can be used as a fallback access mechanism while you configure and test certificate authentication. After you configure certificate authentication, you may choose to disable forms-based log on and password authentication to rely on your public key infrastructure for all log on requests. To disable forms-based log on entirely, add or edit the following value in the Manager.properties configuration file:

```
com.vontu.manager.form authentication = false
```

See "Configuring certificate authentication for the Enforce Server administration console" on page 112.

You must stop and then restart the Vontu Manager service to apply your changes.

Note: Disabling forms-based log on disables the feature for all users, including those with Administrator privileges. As an alternative, you can disable forms-based log on or certificate authentication for an individual user by configuring that user's account.

See "Configuring user accounts" on page 99.

If you later turn on forms-based log on but the Administrator user account does not have a password configured, you can reset the Administrator password using the AdminPasswordReset utility.

See "Resetting the Administrator password" on page 103.

Chapter 6

# Connecting to group directories

This chapter includes the following topics:

- Creating connections to LDAP servers
- Configuring directory server connections
- Scheduling directory server indexing

# **Creating connections to LDAP servers**

Symantec Data Loss Prevention supports directory server connections to LDAP-compliant directory servers such as Microsoft Active Directory (AD). A group directory connection specifies how the Enforce Server or Discover Server connects to the directory server.

The connection to the directory server must be established before you create any user groups in the Enforce Server. The Enforce Server or Discover Server uses the connection to obtain details about the groups. If this connection is not created, you are not able to define any **User Groups**. The connection is not permanent, but you can configure the connection to synchronize at a specified interval. The directory server contains all of the information that you need to create **User Groups**.

See "User Groups" on page 292.

**Note:** If you use a directory server that contains a self-signed authentication certificate, you must add the certificate to the Enforce Server or the Discover Server. If your directory server uses a pre-authorized certificate, it is automatically added to the Enforce Server or Discover Server. See "Importing SSL certificates to Enforce or Discover servers" on page 197.

### To create a group directory connection

- 1 Navigate to the **System > Settings > Directory Connections** screen.
- 2 Click Add Connection.
- **3** Configure the directory connection.

See "Configuring directory server connections" on page 127.

# **Configuring directory server connections**

The **Directory Connections** page is the home page for configuring directory server connections. Once you define the directory connection, you can create one or more User Groups.

See "Configuring User Groups" on page 654.

Configuring directory server connections Table 6-1

Step	Action	Description
1	Navigate to the <b>Directory Connections</b> page (if not already there).	This page is available at System > Settings > Directory Connections.
2	Click Create New Connection.	This action takes you to the Configure Directory Connection page.
3	Enter a <b>Name</b> for the directory server connection.	The <b>Connection Name</b> is the user-defined name for the connection. It appears at the <b>Directory Connections</b> home page once the connection is configured.
4	Specify the <b>Network Parameters</b> for the directory server connection.	Table 6-2 provides details on these parameters.  Enter or specify the following parameters:  The Hostname of the computer where the directory server is installed.  The Port on the directory server that supports connections.  The Base DN (distinguished name) of the directory server.  The Encryption Method for the connection, either None or Secure.
5	Specify the <b>Authentication</b> mode for connecting to the directory server.	Table 6-3 provides details on configuring the authentication parameters.
6	Click <b>Test Connection</b> to verify the connection.	If there is anything wrong with the connection, the system displays an error message describing the problem.

Configuring directory server connections (continued) Table 6-1

Step	Action	Description
7	Click <b>Save</b> to save the direction connection configuration.	The system automatically indexes the directory server after you successfully create, test, and save the directory server connection.
8	Select the Index and Replication Status tab.	Verify that the directory server was indexed. After some time (depending on the size of the directory server query), you should see that the <b>Replication Status</b> is "Completed <date> <ti>If you do not see that the status is completed, verify that you have configured and tested the directory connection properly. Contact your directory server administrator for assistance.</ti></date>
9	Select the <b>Index Settings</b> tab.	You can adjust the directory server indexing schedule as necessary at the <b>Index Settings</b> tab.  See "Scheduling directory server indexing" on page 129.

Directory connection network parameters Table 6-2

Network parameters	Description	
Hostname	Enter the <b>Hostname</b> of the directory server.	
	For example: enforce.dlp.symantec.com	
	You must enter the Fully Qualified Name (FQN) of the directory server. Do not use the IP address.	
Port	Enter the connection <b>Port</b> for the directory server.	
	For example: 389	
	Typically the port is 389 or 636 for secure connections.	
Base DN	Enter the <b>Base DN</b> for the directory server. This field only accepts one directory server entry.	
	For example: dc=enforce, dc=dlp, dc=symantec, dc=com	
	The Base DN string cannot contain any space characters.	
	The <b>Base DN</b> is the base distinguished name of the directory server. Typically, this name is the domain name of the directory server. The Base DN parameter defines the initial depth of the directory server search.	

Table 6-2 Directory connection network parameters (continued)

Network parameters	Description
Encryption Method	Select the <b>Secure</b> option if you want the communication between the directory server and the Enforce Server to be encrypted using SSL.
	<b>Note:</b> If you choose to use a secure connection, you may need to import the SSL certificate for the directory server to the Enforce Server keystore. See "Importing SSL certificates to Enforce or Discover servers" on page 197.

Table 6-3 Directory connection authentication parameters

Authentication	Description
Authentication	Select the <b>Authentication</b> option to connect to the directory server using authentication mode. Check <b>Connect with Credentials</b> to add your username and password to authenticate to the directory server.
Username	To authenticate with Active Directory, use one of the following methods:  Domain and user name, for example: Domain\username  User name and domain, for example: username@domain.com  Fully distinguished user name and domain (without spaces), for example: cn=username, cn=Users, dc=domain, dc=com  To authenticate with another type of directory server:  A different syntax may be required, for example: uid=username, ou=people, o=company
Password	Enter the password for the user name that was specified in the preceding field.  The password is obfuscated when you enter it.

# Scheduling directory server indexing

Each directory connection is set to automatically index the configured LDAP server **once** at 12:00 AM the day after you create the initial connection. You can modify the indexing schedule to specify when and how often the index is synchronized.

Each directory server connection is set to automatically index the configured User Groups hosted in the directory server **once** at 12:00 AM the day after you create the initial connection.

After you create, test, and save the directory server connection, the system automatically indexes all of the User Groups that are hosted in the directory whose connection you have established. You can modify this setting, and schedule indexing daily, weekly, or monthly.

### To schedule group directory indexing

1 Select an existing group directory server connection from the System > **Settings > Directory Connections** screen. Or, create a new connection.

See "Configuring directory server connections" on page 127.

2 Adjust the Index Settings to the desired schedule.

See Table 6-4 on page 130.

Schedule group directory server indexing and view status Table 6-4

Index Settings	Description	
Index the directory server once.	The <b>Once</b> setting is selected by default and automatically indexes the director server at 12:00 AM the day after you create the initial connection.	
	You can modify the default <b>Once</b> indexing schedule by specifying when and how often the index is supposed to be rebuilt.	
Index the directory	Select the <b>Daily</b> option to schedule the index daily.	
server daily.	Specify the <b>time of day</b> and, optionally, the <b>Until</b> duration for this schedule.	
Index the directory server weekly.	Select the <b>Weekly</b> option to schedule the index to occur once a week.	
	Specify the day of the week to index.	
	Specify the <b>time</b> to index.	
	Optionally, specify the <b>Until</b> duration for this schedule.	
Index the directory	Specify the <b>day of the month</b> to index the directory and the <b>time</b> .	
server monthly.	Optionally, specify the Until duration for this schedule.	
View the indexing and replication status.	Select the <b>Index and Replication Status</b> tab to view the status of the indexing process.	
	■ Indexing Status	
	Displays the next scheduled index, date and time.  Detection Server Name	
	Displays the detection server where the User Group profile is deployed.	
	■ Replication Status	
	<ul> <li>Displays the data and time of the most recent synchronization with the directory group server.</li> </ul>	

Chapter 7

# Managing stored credentials

This chapter includes the following topics:

- About the credential store
- Adding new credentials to the credential store
- Configuring endpoint credentials
- Managing credentials in the credential store

## About the credential store

An authentication credential can be stored as a named credential in a central credential store. It can be defined once, and then referenced by any number of Discover targets. Passwords are encrypted before they are stored.

The credential store simplifies management of user name and password changes.

You can add, delete, or edit stored credentials.

See "Adding new credentials to the credential store" on page 132.

See "Managing credentials in the credential store" on page 133.

The Credential Management screen is accessible to users with the "Credential Management" privilege.

Stored credentials can be used when you edit or create a Discover target.

See "Network Discover scan target configuration options" on page 1191.

# Adding new credentials to the credential store

You can add new credentials to the credential store. These credentials can later be referenced with the credential name.

### To add a stored credential

1 Click System > Settings > Credentials, and click Add Credential.

2 Enter the following information:

> Credential Name Enter your name for this stored credential.

> > The credential name must be unique within the credential store. The name is used only

to identify the credential.

Access Username Enter the user name for authentication.

Access Password Enter the password for authentication.

Re-enter Access Password Re-enter the password.

Click Save.

You can later edit or delete credentials from the credential store.

See "Managing credentials in the credential store" on page 133.

See "Configuring endpoint credentials" on page 132.

# Configuring endpoint credentials

You must add credentials to the Credential Store before you can access credentials for Endpoint FlexResponse or the Endpoint Discover Quarantine response rule. The credentials are stored in an encrypted folder on all endpoints that are connected to an Endpoint Server. Because all endpoints store the credentials, you must be careful about the type of credentials you store. Use credentials that cannot access other areas of your system. Before your endpoint credentials can be used, you must enable the Enforce Server to recognize them.

### To create endpoint credentials

- 1 Go to: System > Settings > General.
- 2 Click Configure.
- 3 Under the Credential Management section, ensure that the Allow Saved Credentials on Endpoint Agent checkbox is selected.

- 4 Click Save.
- 5 Go to: System > Settings > Credentials.
- Click Add Credential.
- 7 Under the **General** section, enter the details of the credential you want to add.
- 8 Under Usage Permission, select Servers and Endpoint agents.
- Click Save.

See "About the credential store" on page 131.

See "Configuring the Endpoint Discover: Quarantine File action" on page 920.

# Managing credentials in the credential store

You can delete or edit a stored credential.

#### To delete a stored credential

- Click **System > Settings > Credentials**. Locate the name of the stored credential that you want to remove.
- Click the delete icon to the right of the name. A credential can be deleted only if it is not currently referenced in a Discover target or indexed document profile.

#### To edit a stored credential

- Click **System > Settings > Credentials**. Locate the name of the stored credential that you want to edit.
- 2 Click the edit icon (pencil) to the right of the name.
- Update the user name or password.
- 4 Click Save.
- If you change the password for a given credential, the new password is used for all subsequent Discover scans that use that credential.

Chapter 8

# Managing system events and messages

This chapter includes the following topics:

- About system events
- System events reports
- Working with saved system reports
- Server event detail
- Configuring event thresholds and triggers
- About system event responses
- Enabling a syslog server
- About system alerts
- Configuring the Enforce Server to send email alerts
- Configuring system alerts
- About log review
- System event codes and messages

## About system events

System events related to your Symantec Data Loss Prevention installation are monitored, reported, and logged.

System event reports are viewed from the Enforce Server administration console:

 The five most recent system events of severity Warning or Severe are listed on the Servers Overview screen (System > Servers > Overview).

See "About the System Overview screen" on page 198.

■ Reports on all system events of any severity can be viewed by going to **System** > Servers > Events.

See "System events reports" on page 135.

 Recent system events for a particular detection server are listed on the Server **Detail** screen for that server.

See "Server Detail screen" on page 201.

 Click on any event in an event list to go to the Event Details screen for that event. The **Event Details** screen provides additional information about the event. See "Server event detail" on page 139.

There are three ways that system events can be brought to your attention:

- System event reports displayed on the administration console
- System alert email messages See "About system alerts" on page 146.
- Syslog functionality See "Enabling a syslog server" on page 144.

Some system events require a response.

See "About system event responses" on page 142.

To narrow the focus of system event management you can:

- Use the filters in the various system event notification methods. See "System events reports" on page 135.
- Configure the system event thresholds for individual servers. See "Configuring event thresholds and triggers" on page 140.

# System events reports

To view all system events, go to the system events report screen (System > Servers > Events). This screen lists events, one event per line. The list contains those events that match the selected data range, and any other filter options that are listed in the Applied Filters bar. For each event, the following information is displayed:

Table 8-1

Events	Description
Туре	The type (severity) of the event. Type may be any one of those listed in Table 8-2.
Time	The date and time of the event.
Server	The name of the server on which the event occurred.
Host	The IP address or host name of the server on which the event occurred.
Code	A number that identifies the kind of event.  See the Symantec Data Loss Prevention Administration Guide for information on event code numbers.
Summary	A brief description of the event. Click on the summary for more detail about the event.

System event types Table 8-2

Event	Description
m	System information
<u> </u>	Warning
⊗	Severe

You can select from several report handling options.

See "Common incident report features" on page 1039.

Click any event in the list to go to the **Event Details** screen for that event. The **Event Details** screen provides additional information about the event.

See "Server event detail" on page 139.

Since the list of events can be long, filters are available to help you select only the events that you are interested in. By default, only the Date filter is enabled and it is initially set to All Dates. The Date filter selects events by the dates the events occurred.

### To filter the list of system events by date of occurrence

- Go to the Filter section of the events report screen and select one of the date range options.
- 2 Click Apply.
- 3 Select **Custom** from the date list to specify beginning and end dates.

In addition to filtering by date range, you can also apply advanced filters. Advanced filters are cumulative with the current date filter. This means that events are only listed if they match the advanced filter and also fall within the current date range. Multiple advanced filters can be applied. If multiple filters are applied, events are only listed if they match all the filters and the date range.

### To apply additional advanced filters

- Click on Advanced Filters and Summarization.
- 2 Click on Add Filter.
- 3 Choose the filter you want to use from the left-most drop-down list. Available filters are listed in Table 8-3.
- Choose the filter-operator from the middle drop-down list.

For each advanced filter you can specify a filter-operator Is Any Of or Is None Of.

- 5 Enter the filter value, or values, in the right-hand text box, or click a value in the list to select it.
  - To select multiple values from a list, hold down the Control key and click each one.
  - To select a range of values from a list, click the first one, then hold down the Shift key and click the last value in the range you want.
- (Optional) Specify additional advanced filters if needed.
- When you have finished specifying a filter or set of filters, click **Apply**. Click the red X to delete an advanced filter.

The **Applied Filters** bar lists the filters that are used to produce the list of events that is displayed. Note that multiple filters are cumulative. For an event to appear on the list it must pass all the applied filters.

The following advanced filters are available:

Table 8-3 System events advanced filter options

Filter	Description
Event Code	Filter events by the code numbers that identify each kind of event. You can filter by a single code number or multiple code numbers separated by commas (2121, 1202, 1204). Filtering by code number ranges, or greater than, or less than operators is not supported.

Filter	Description
Event type	Filter events by event severity type (Info, Warning, or Severe).
Server	Filter events by the server on which the event occurred.

Table 8-3 System events advanced filter options (continued)

Note: A small subset of the parameters that trigger system events have thresholds that can be configured. These parameters should only be adjusted with advice from Symantec Support. Before changing these settings, you should have a thorough understanding of the implications that are involved. The default values are appropriate for most installations.

See "Configuring event thresholds and triggers" on page 140.

See "About system events" on page 134.

See "Server event detail" on page 139.

See "Working with saved system reports" on page 138.

See "Configuring event thresholds and triggers" on page 140.

See "About system alerts" on page 146.

# Working with saved system reports

The System Reports screen lists system and agent-related reports that have previously been saved. To display the System Reports screen, click System > **System Reports**. Use this screen to work with saved system reports.

### To create a saved system report

- 1 Go to one of the following screens:
  - System Events (System > Events)
  - Agents Overview (System > Agents > Overview)
  - Agents Events (System > Agents > Events)

See "About the Enforce Server administration console" on page 56.

2 Select the filters and summaries for your custom report.

See "About custom reports and dashboards" on page 1019.

3 Select Report > Save As. Enter the saved report information.

See "Saving custom incident reports" on page 1022.

5 Click Save.

The **System Reports** screen is divided into two sections:

- System Event Saved Reports lists saved system reports.
- Agent Management Saved Reports lists saved agent reports.

For each saved report you can perform the following operations:

- Share the report. Click share to allow other Symantec Data Loss Prevention uses who have the same role as you to share the report. Sharing a report cannot be undone; after a report is shared it cannot be made private. After a report is shared, all users with whom it is shared can view, edit, or delete the report. See "Saving custom incident reports" on page 1022.
- Change the report name or description. Click the pencil icon to the right of the report name to edit it.
- Change the report scheduling. Click the calendar icon to the right of the report name to edit the delivery schedule of the report and to whom it is sent. See "Saving custom incident reports" on page 1022. See "Delivery schedule options for incident and system reports" on page 1025.
- Delete the report. Click the red X to the right of the report name to delete the report.

## Server event detail

The Server Event Detail screen is reached by System > Servers > Events and then clicking on one of the listed events.

See "System events reports" on page 135.

The Server Event Detail screen displays all of the information available for the selected event. None of the information on this screen is editable.

The Server Event Detail screen is divided into two sections—General and Message.

1 abie 0-4	Event detail — deficial
Item	Description
Туре	The event is one of the following types:  Info: Information about the system.  Warning: A problem that is not severe enough to generate an error.  Severe: An error that requires immediate attention.
Time	The date and time of the event.
Server	The name of the server.
Host	The host name or IP address of the server.

Table 8-/ Event detail — General

**Table 8-5** Event detail — Message

Item	Description
Code	A number that identifies the kind of event.
	See "System event codes and messages" on page 150.
Summary	A brief description of the event.
Detail	Detailed information about the event.

See "About system events" on page 134.

See "Server event detail" on page 139.

See "System events reports" on page 135.

See "About system alerts" on page 146.

# Configuring event thresholds and triggers

A small subset of the parameters that trigger system events have thresholds that can be configured. These parameters are configured for each detection server separately. These parameters should only be adjusted with advice from Symantec Support. Before changing these settings, you should have a thorough understanding of the implications. The default values are appropriate for most installations.

See "About system events" on page 134.

To view and change the configurable parameters that trigger system events

- 1 Go to the Server Overview screen (System > Servers > Overview).
- 2 Click on the name of a detection server to display that server's Server Detail screen.
- 3 Click the Server Settings tab.

The Advanced Server Settings screen for that server is displayed.

4 Change the configurable parameters, as needed.

Table 8-6 Configurable parameters that trigger events

Parameter	Description	Event
BoxMonitor.DiskUsageError	Indicates the amount of filled disk space (as a percentage) that triggers a severe system event. For example, a Severe event occurs if a detection server is installed on the C drive and the disk space error value is 90. The detection server creates a Severe system event when the C drive usage is 90% or greater. The default is 90.	Low disk space
BoxMonitor.DiskUsageWarning	Indicates the amount of filled disk space (as a percentage) that triggers a Warning system event. For example, a Warning event occurs if the detection server is installed on the C drive and the disk space warning value is 80. Then the detection server generates a Warning system event when the C drive usage is 80% or greater. The default is 80.	Low disk space
BoxMonitor.MaxRestartCount	Indicates the number of times that a system process can be restarted in one hour before a Severe system event is generated. The default is 3.	process name restarts excessively
IncidentDetection.MessageWaitSevere	Indicates the number of minutes messages need to wait to be processed before a Severe system event is sent about message wait times. The default is 240.	Long message wait time

Table 8-6Configurable parameters that trigger events (continued)		gger events (continued)
Parameter	Description	Event
IncidentDetection.MessageWaitWarning	Indicates the number of minutes messages need to wait to be processed before sending a Severe system event about message wait times. The default is 60.	Long message wait time
IncidentWriter.BacklogInfo	Indicates the number of incidents that can be queued before an Info system event is generated. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have slowed down or stopped. The default is 1000.	N incidents in queue
IncidentWriter.BacklogWarning	Indicates the number of incidents that can be queued before generating a Warning system event. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have slowed down or stopped. The default is 3000.	N incidents in queue
IncidentWriter.BacklogSevere	Indicates the number of incidents that can be queued before a Severe system event is generated. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have	N incidents in queue

# About system event responses

There are three ways that system events can be brought to your attention:

System event reports displayed on the administration console

slowed down or stopped. The default is

 System alert email messages See "About system alerts" on page 146.

10000.

 Syslog functionality See "Enabling a syslog server" on page 144. In most cases, the system event summary and detail information should provide enough information to direct investigation and remediation steps. The following table provides some general guidelines for responding to system events.

System event responses Table 8-7

System Event or Category	Appropriate Response
Low disk space	If this event is reported on a detection server, recycle the Symantec Data Loss Prevention services on the detection server. The detection server may have lost its connection to the Enforce Server. The detection server then queues its incidents locally, and fills up the disk.
	If this event is reported on an Enforce Server, check the status of the Oracle and the Vontu Incident Persister services. Low disk space may result if incidents do not transfer properly from the file system to the database. This event may also indicate a need to add additional disk space.
Tablespace is almost full	Add additional data files to the database. When the hard disk is at 80% of capacity, obtain a bigger disk instead of adding additional data files.
	Refer to the Symantec Data Loss Prevention Installation Guide.
Licensing and versioning	Contact Symantec Support.
Monitor not responding	Restart the Symantec Monitor service. If the event persists, check the network connections. Make sure the computer that hosts the detections server is turned on by connecting to it. You can connect with terminal services or another remote desktop connection method. If necessary, contact Symantec Support.  See "About Data Lost Prevention services" on page 76.
Alert or scheduled report sending failed	Go to <b>System &gt; Settings &gt; General</b> and ensure that the settings in the Reports and Alerts and SMTP sections are configured correctly. Check network connectivity between the Enforce Server and the SMTP server. Contact Symantec Support.
Auto key ignition failed	Contact Symantec Support.

Table 8-7 System event responses (continued)

System Event or Category	Appropriate Response
Cryptographic keys are inconsistent	Contact Symantec Support.
Long message wait time	Increase detection server capacity by adding more CPUs or replacing the computer with a more powerful one.
	Decrease the load on the detection server. You can decrease the load by applying the traffic filters that have been configured to detect fewer incidents. You can also re-route portions of the traffic to other detection servers.
	Increase the threshold wait times if all of the following items are true:
	<ul> <li>This message is issued during peak hours.</li> <li>The message wait time drops down to zero before the next peak.</li> <li>The business is willing to have such delays in</li> </ul>
	message processing.
process_name restarts excessively	Check the process by going to <b>System &gt; Servers</b> > <b>Overview</b> . To see individual processes on this screen, Process Control must be enabled by going to <b>System &gt; Settings &gt; General &gt; Configure</b> .
N incidents in queue	Investigate the reason for the incidents filling up the queue.
	The most likely reasons are as follows:
	<ul> <li>Connection problems. Response: Make sure the communication link between the Endpoint Server and the detection server is stable.</li> <li>Insufficient connection bandwidth for the number of generated incidents (typical for WAN connections). Response: Consider changing policies (by configuring the filters) so that they generate fewer incidents.</li> </ul>

# **Enabling a syslog server**

Syslog functionality sends Severe system events to a syslog server. Syslog servers allow system administrators to filter and route the system event notifications on a more granular level. System administrators who use syslog regularly for monitoring their systems may prefer to use syslog instead of alerts. Syslog may be preferred if the volume of alerts seems unwieldy for email.

Syslog functionality is an on or off option. If syslog is turned on, all Severe events are sent to the syslog server.

#### To enable syslog functionality

- Go to the \SymantecDLP\Protect\config directory on Windows or the /opt/SymantecDLP/Protect/config directory on Linux.
- 2 Open the Manager.properties file.
- 3 Uncomment the #systemevent.syslog.host= line by removing the # symbol from the beginning of the line, and enter the hostname or IP address of the syslog server.
- Uncomment the #systemevent.syslog.port= line by removing the # symbol from the beginning of the line. Enter the port number that should accept connections from the Enforce Server server. The default is 514.
- 5 Uncomment the #systemevent.syslog.format= [{0}] {1} - {2} line by removing the # symbol from the beginning of the line. Then define the system event message format to be sent to the syslog server:

If the line is uncommented without any changes, the notification messages are sent in the format: [server name] summary - details. The format variables are:

- {0} the name of the server on which the event occurred
- {1} the event summary
- {2} the event detail

For example, the following configuration specifies that Severe system event notifications are sent to a syslog host named server1 which uses port 600.

```
systemevent.syslog.host=server1
systemevent.syslog.port=600
systemevent.syslog.format= [{0}] {1} - {2}
```

Using this example, a low disk space event notification from an Enforce Server on a host named dlp-1 would look like:

```
dlp-1 Low disk space - Hard disk space for
incident data storage server is low. Disk usage is over 82%.
```

See "About system events" on page 134.

## About system alerts

System alerts are email messages that are sent to designated addresses when a particular system event occurs. You define what alerts (if any) that you want to use for your installation. Alerts are specified and edited on the Configure Alert screen, which is reached by System > Servers > Alerts > Add Alert.

Alerts can be specified based on event severity, server name, or event code, or a combination of those factors. Alerts can be sent for any system event.

The email that is generated by the alert has a subject line that begins with Symantec Data Loss Prevention System Alert followed by a short event summary. The body of the email contains the same information that is displayed by the Event **Detail** screen to provide complete information about the event.

See "Configuring the Enforce Server to send email alerts" on page 146.

See "Configuring system alerts" on page 147.

See "Server event detail" on page 139.

## Configuring the Enforce Server to send email alerts

To send out email alerts regarding specified system events, the Enforce Server has to be configured to support sending of alerts and reports. This section describes how to specify the report format and how to configure Symantec Data Loss Prevention to communicate with an SMTP server.

After completing the configuration described here, you can schedule the sending of specific reports and create specific system alerts.

To configure Symantec Data Loss Prevention to send alerts and reports

- 1 Go to System > Settings > General and click Configure. The **Edit General Settings** screen is displayed.
- In the **Reports and Alerts** section, select one of the following distribution methods:
  - Send reports as links, logon is required to view. Symantec Data Loss Prevention sends email messages with links to reports. You must log on to the Enforce Server to view the reports.

Note: Reports with incident data cannot be distributed if this option is set.

**Send report data with emails**. Symantec Data Loss Prevention sends email messages and attaches the report data.

Enter the Enforce Server domain name or IP address in the Fully Qualified Manager Name field.

If you send reports as links, Symantec Data Loss Prevention uses the domain name as the basis of the URL in the report email.

Do not specify a port number unless you have modified the Enforce Server to run on a port other than the default of 443.

If you want alert recipients to see any correlated incidents, check the Correlations Enabled box.

When correlations are enabled, users see them on the **Incident Snapshot** screen.

In the **SMTP** section, identify the SMTP server to use for sending out alerts and reports.

Enter the relevant information in the following fields:

- Server: The fully qualified hostname or IP address of the SMTP server that Symantec Data Loss Prevention uses to deliver system events and scheduled reports.
- System email: The email address for the alert sender. Symantec Data Loss Prevention specifies this email address as the sender of all outgoing email messages. Your IT department may require the system email to be a valid email address on your SMTP server.
- User ID: If your SMTP server requires it, type a valid user name for accessing the server. For example, enter DOMAIN\bsmith.
- Password: If your SMTP server requires it, enter the password for the User ID.

#### Click Save.

See "About system alerts" on page 146.

See "Configuring system alerts" on page 147.

See "About system events" on page 134.

## Configuring system alerts

You can configure Symantec Data Loss Prevention to send an email alert whenever it detects a specified system event. Alerts can be specified based on event severity, server name, or event code, or a combination of those factors. Alerts can be sent for any system event.

See "About system alerts" on page 146.

Note that the Enforce Server must first be configured to send alerts and reports.

See "Configuring the Enforce Server to send email alerts" on page 146.

Alerts are specified and edited on the Configure Alert screen, which is reached by System > Servers > Alerts and then choosing Add Alert to create a new alert, or clicking on the name of an existing alert to modify it.

#### To create or modify an alert

- 1 Go the Alerts screen (System > Servers > Alerts).
- 2 Click the Add Alert tab to create a new alert, or click on the name of an alert to modify it.
  - The Configure Alert screen is displayed.
- 3 Fill in (or modify) the name of the alert. The alert name is displayed in the subject line of the email alert message.
- 4 Fill in (or modify) a description of the alert.
- 5 Click **Add Condition** to specify a condition that will trigger the alert.
  - Each time you click **Add Condition** you can add another condition. If you specify multiple conditions, every one of the conditions must be met to trigger the alert.
  - Click on the red X next to a condition to remove it from an existing alert.
- Enter the email address that the alert is to be sent to. Separate multiple addresses by commas.
- Limit the maximum number of times this alert can be sent in one hour by entering a number in the Max Per Hour box.
  - If no number is entered in this box, there is no limit on the number of times this alert can be sent out. The recommended practice is to limit alerts to one or two per hour, and to substitute a larger number later if necessary. If you specify a large number, or no number at all, recipient mailboxes may be overloaded with continual alerts.
- Click Save to finish.

The Alerts list is displayed.

There are three kinds of conditions that you can specify to trigger an alert:

- Event type the severity of the event.
- Server the server associated with the event.
- Event code a code number that identifies a particular kind of event.

For each kind of condition, you can choose one of two operators:

- Is any of.
- Is none of.

For each kind of condition, you can specify appropriate parameters:

- Event type. You can select one, or a combination of, **Information**, **Warning**, Severe. Click on an event type to specify it. To specify multiple types, hold down the Control key while clicking on event types. You can specify one, two, or all three types.
- Server. You can select one or more servers from the list of available servers. Click on the name of server to specify it. To specify multiple servers, hold down the Control key while clicking on server names. You can specify as many different servers as necessary.
- Event code. Enter the code number. To enter multiple code numbers, separate them with commas or use the Return key to enter each code on a separate line. See "System event codes and messages" on page 150.

By combining multiple conditions, you can define alerts that cover a wide variety of system conditions.

Note: If you define more than one condition, the conditions are treated as if they were connected by the Boolean "AND" operator. This means that the Enforce Server only sends the alert if all conditions are met. For example, if you define an event type condition and a server condition, the Enforce Server only sends the alert if the specified event occurs on the designated server.

See "About system alerts" on page 146.

See "Configuring the Enforce Server to send email alerts" on page 146.

See "System events reports" on page 135.

## **About log review**

Your Symantec Data Loss Prevention installation includes a number of log files. These files provide information on server communication, Enforce Server and detection server operation, incident detection, and so on.

By default, logs for the Enforce Server and detection server are stored in the following directories:

- Windows:SymantecDLP\Protect\logs
- Linux: /var/log/SymantecDLP

See "About log files" on page 243.

See also the Symantec Data Loss Prevention System Maintenance Guide for additional information about working with logs.

## System event codes and messages

Symantec Data Loss Prevention system events are monitored, reported, and logged. Each event is identified by code number listed in the tables.

See "About system events" on page 134.

System event lists and reports can be filtered by event codes.

See "System events reports" on page 135.

Note: Numbers enclosed in braces, such as {0}, indicate text strings that are dynamically inserted into the actual event name or description message.

Table 8-8 General detection server events

Code	Summary	Description
1000	Monitor started	All monitor processes have been started.
1001	Local monitor started	All monitor processes have been started.
1002	Monitor started	Some monitor processes are disabled and haven't been started.
1003	Local monitor started	Some monitor processes are disabled and haven't been started.
1004	Monitor stopped	All monitor processes have been stopped.
1005	Local monitor stopped	All monitor processes have been stopped.
1006	{0} failed to start	Process {0} can't be started. See log files for more detail.
1007	{0} restarts excessively	Process {0} has restarted {1} times during last {2} minutes.
1008	{0} is down	{0} process went down before it had fully started.
1010	Restarted {0}	{0} process was restarted because it went down unexpectedly.
1011	Restarted {0}	{0} was restarted because it was not responding.
1012	Unable to start {0}	Cannot bind to the shutdown datagram socket. Will retry.
1013	{0} resumed starting	Successfully bound to the shutdown socket.

General detection server events (continued) Table 8-8

Code	Summary	Description
1014	Low disk space	Hard disk space is low. Symantec Data Loss Prevention server disk usage is over {0}%.

Table 8-9 **Endpoint server events** 

Code	Summary	Description
1100	Aggregator started	None
1101	Aggregator failed to start	Error starting Aggregator. {0} No incidents will be detected.
1102	Communications with non-legacy agents are disabled	SSL keystore and truststore are not configured for this endpoint server. Please go to configure server page to configure SSL keystore and truststore.

**Table 8-10** Detection configuration events

Code	Summary	Description
1200	Loaded policy	"{0}" Policy "{0}" v{1} ({2}) has been successfully loaded.
1201	Loaded policies {0}	None
1202	No policies loaded	No relevant policies are found. No incidents will be detected. 1203 Unloaded policy "{0}" Policy "{0}" has been unloaded.
1204	Updated policy "{0}"	Policy "{0}" has been successfully updated. The current policy version is {1}. Active channels: {2}.
1205	Incident limit reached for Policy "{0}"	The policy "{0}" has found incidents in more than {1} messages within the last {2} hours. The policy will not be enforced until the policy is changed, or the reset period of {2} hours is reached.
1206	Long message wait time	Message wait time was {0}:{1}:{2}:{3}.
1207	Failed to load Vector Machine Learning profile	Failed to load [{0}] Vector Machine Learning profile. See server logs for more details.
1208	Failed to unload Vector Machine Learning profile	Failed to unload [{0}] Vector Machine Learning profile. See server logs for more details.
1209	Loaded Vector Machine Learning profile	Loaded [{0}] Vector Machine Learning profile.

Detection configuration events (continued) **Table 8-10** 

Code	Summary	Description
1210	Unloaded Vector Machine Learning profile	Unloaded [{0}] Vector Machine Learning profile.
1211	Vector Machine Learning training successful	Training succeeded for [{0}] Vector Machine Learning profile.
1212	Vector Machine Learning training failed	Training failed for [{0}] Vector Machine Learning profile.
1213	{0} messages timed out in Detection recently	{0} messages timed out in Detection in the last {1} minutes. Enable Detection execution trace logs for details.

**Table 8-11** File reader events

Code	Summary	Description
1301	File Reader started	None
1302	File Reader failed to start	Error starting File Reader. {0} No incidents will be detected.
1303	Unable to delete folder	File Reader was unable to delete folder "{0}" in the file system. Please investigate, as this will cause system malfunction.
1304	Channel enabled	Monitor channel "{0}" has been enabled.
1305	Channel disabled	Monitor channel "{0}" has been disabled. 1306 License received. {0}.
1306	License received.	None
1307	started	Process is started.
1308	down	Process is down.

ICAP events **Table 8-12** 

Code	Summary	Description
1400	ICAP channel configured	The channel is in {0} mode
1401	Invalid license	The ICAP channel is not licensed or the license has expired. No incidents will be detected or prevented by the ICAP channel.

ICAP events (continued) **Table 8-12** 

Code	Summary	Description
1402	Content Removal Incorrect	Configuration rule in line {0} is outdated or not written in proper grammar format. Either remove it from the config file or update the rule.
1403	Out of memory Error (Web Prevent) while processing message	While processing request on connection ID{0}, out of memory error occurred. Please tune your setup for traffic load.
1404	Host restriction	Any host (ICAP client) can connect to ICAP Server.
1405	Host restriction error	Unable to get the IP address of host {0}.
1406	Host restriction error	Unable to get the IP address of any host in Icap.AllowHosts.
1407	Protocol Trace Enabled	Enabled Traces available at {0}.
1408	Invalid Load Balance Factor Icap	LoadBalanceFactor configured to 0. Treating it as 1.

**Table 8-13** MTA events

Code	Summary	Description
1500	Invalid license	The SMTP Prevent channel is not licensed or the license has expired. No incidents will be detected or prevented by the SMTP Prevent channel.
1501	Bind address error	Unable to bind {0}. Please check the configured address or the RequestProcessor log for more information. 1502 MTA restriction error Unable to resolve host {0}.
1503	All MTAs restricted	Client MTAs are restricted, but no hosts were resolved. Please check the RequestProcessor log for more information and correct the RequestProcessor.AllowHosts setting for this Prevent server.
1504	Downstream TLS Handshake failed	TLS handshake with downstream MTA {0} failed. Please check SmtpPrevent and RequestProcessor logs for more information.
1505	Downstream TLS Handshake successful	TLS handshake with downstream MTA {0} was successfully completed.

**Table 8-14** File inductor events

Code	Summary	Description
1600	Override folder invalid	Monitor channel {0} has invalid source folder: {1} Using folder: {2}.
1601	Source folder invalid	Monitor channel {0} has invalid source folder: {1} The channel is disabled.

**Table 8-15** File scan events

Code	Summary	Description
1700	Scan start failed	Discover target with ID {0} does not exist. 1701 Scan terminated {0}
1702	Scan completed	Discover target "{0}" completed a scan successfully.
1703	Scan start failed	{0}
1704	Share list had errors	{0}
1705	Scheduled scan failed	Failed to start a scheduled scan of Discover target {0}. {1}
1706	Scan suspend failed	{0}
1707	Scan resume failed	{0}
1708	Scheduled scan suspension failed	Scheduled suspension failed for scan of Discover target {0}. {1}
1709	Scheduled scan resume failed	Scheduled suspension failed for scan of Discover target {0}. {1}
1710	Maximum Scan Duration Timeout Occurred	Discover target "{0}" timed out because of Maximum Scan Duration.
1711	Maximum Scan Duration Timeout Failed	Maximum scan time duration timed out for scan: {0}. However, an error occurred while trying to abort the scan.
1712	Scan Idle Timeout Occurred	Discover target "{0}" timed out because of Scan Idle Timeout.
1713	Scan Idle Timeout Failed	Maximum idle time duration timed out for scan: {0}. However, an error occurred while trying to abort the scan.
1714	Scan terminated - Invalid Server State	Scan of discover target "{0}" has been terminated from the state of "{1}" because the associated discover server {2} entered an unexpected state of "{3}".

File scan events (continued) **Table 8-15** 

Code	Summary	Description
1715	Scan terminated - Server Removed	Scan of discover target "{0}" has been terminated because the associated discover server {1} is no longer available.
1716	Scan terminated - Server Reassigned	Scan of discover target "{0}" has been terminated because the associated discover server {1} is already scanning discover target(s) "{2}".
1717	Scan terminated - Transition Failed	Failed to handle the state change of discover server {1} while scanning discover target "{0}". See log files for details.
1718	Scan start failed	Scan of discover target "{0}" has failed to start. See log files for detailed error description.
1719	Scan start failed due to unsupported target type	Scan of discover target "{0}" has failed, as its target type is no longer supported.

**Table 8-16** Incident persister and incident writer events

Code	Summary	Description
1800	Incident Persister is unable to process incident Incident	Persister ran out of memory processing incident {0}.
1801	Incident Persister failed to process incident {0}	
1802	Corrupted incident received	A corrupted incident was received, and renamed to {0}.
1803	Policy misconfigured	Policy "{0}" has no associated severity.
1804	Incident Persister is unable to start	Incident Persister cannot start because it failed to access the incident folder {0}. Check folder permissions.
1805	Incident Persister is unable to access	Incidents folder The Incident Persister is unable to access the incident folder {0}. Check folder permissions.
1806	Response rule processing failed to start	Response rule processing failed to start: {0}.
1807	Response rule processing execution failed	Response rule command runtime execution failed from error: {0}.
1808	Unable to write incident	Failed to delete old temporary file {0}.
1809	Unable to write incident	Failed to rename temporary incident file {0}.

**Table 8-16** Incident persister and incident writer events (continued)

Code	Summary	Description
1810	Unable to list incidents	Failed to list incident files in folder {0}. Check folder permissions.
1811	Error sending incident	Unexpected error occurred while sending an incident. {0} Look in the incident writer log for more information.
1812	Incident writer stopped	Failed to delete incident file {0} after it was sent. Delete the file manually, correct the problem and restart the incident writer.
1813	Failed to list incidents	Failed to list incident files in folder {0}. Check folder permissions.
1814	Incident queue backlogged	There are {0} incidents in this server's queue.
1815	Low disk space on incident server	Hard disk space for the incident data storage server is low. Disk usage is over {0}%.
1816	Failed to update policy statistics	Failed to update policy statistics for policy {0}.
1817	Daily incident maximum exceeded	The daily incident maximum for policy {0} has been exceeded.\n No further incidents will be generated.
1818	Incident is oversized, has been persisted with a limited number of components and/or violations	Incident is oversized, has been partially persisted with messageID {0}, Incident File Name {1}.

**Table 8-17** Install or update events

Code	Summary	Description
1900	Failed to load update package	Database connection error occurred while loading the software update package {0}.
1901	Software update failed	Failed to apply software update from package {0}. Check the update service log.

Key ignition password events **Table 8-18** 

Code	Summary	Description
2000	Key ignition error	Failed to ignite keys with the new ignition password. Detection against Exact Data Profiles will be disabled.

Key ignition password events (continued) **Table 8-18** 

Code	Summary	Description
2001	Unable to update key ignition password.	The key ignition password won't be updated, because the cryptographic keys aren't ignited. Exact Data Matching will be disabled.

Admin password reset event code **Table 8-19** 

Code	Summary	Description
2099	Administrator password reset	The Administrator password has been reset by the password reset tool.

**Table 8-20** Manager administrator and policy events

Code	Summary	Description
2100	Administrator saved	The administrator settings were successfully saved.
2101	Data source removed	The data source with ID {0} was removed by {1}.
2102	Data source saved	The {0} data source was saved by {1}.
2103	Document source removed	The document source with ID {0} was removed by {1}.
2104	Document source saved	The {0} document source was saved by {1}.
2105	New protocol created	The new protocol {0} was created by {1}.
2106	Protocol order changed	The protocol {0} was moved {1} by {2}.
2107	Protocol removed	The protocol {0} was removed by {1}.
2108	Protocol saved	The protocol {0} was edited by {1}.
2109	User removed	The user with ID {0} was removed by {1}.
2110	User saved	The user {0} was saved by {1}.
2111	Runaway lookup detected	One of the attribute lookup plug-ins did not complete gracefully and left a running thread in the system. Manager restart may be required for cleanup.
2112	Loaded Custom	Attribute Lookup Plug-ins The following Custom Attribute Lookup Plug-ins were loaded: {0}.
2113	No Custom Attribute Lookup Plug-in was loaded	No Custom Attribute Lookup Plug-in was found.

Manager administrator and policy events (continued) **Table 8-20** 

Code	Summary	Description
2114	Custom attribute lookup failed	Lookup plug-in {0} timed out. It was unloaded.
2115	Custom attribute lookup failed	Failed to instantiate lookup plug-in {0}. It was unloaded. Error message: {1}
2116	Policy changed	The {0} policy was changed by {1}.
2117	Policy removed	The {0} policy was removed by {1}.
2118	Alert or scheduled report sending failed. {0}	configured by {1} contains the following unreachable email addresses: {2}. Either the addresses are bad or your email server does not allow relay to those addresses.
2119	System settings changed	The system settings were changed by {0}.
2120	Endpoint Location settings changed	The endpoint location settings were changed by {0}.
2121	The account "{1}" has been locked out	The maximum consecutive failed logon number of {0} attempts has been exceeded for account "{1}", consequently it has been locked out.
2122	Loaded FlexResponse Actions	The following FlexResponse Actions were loaded: {0}.
2123	No FlexResponse Action was loaded.	No FlexResponse Action was found.
2124	A runaway FlexResponse action was detected.	One of the FlexResponse plug-ins did not complete gracefully and left a running thread in the system. Manager restart may be required for cleanup.
2125	Data Insight settings changed.	The Data Insight settings were changed by {0}.
2126	Agent configuration created	Agent configuration {0} was created by {1}.
2127	Agent configuration modified	Agent configuration {0} was modified by {1}.
2128	Agent configuration removed	Agent configuration {0} was removed by {1}.
2129	Agent configuration applied	Agent configuration {0} was applied to endpoint server {1} by {2}.
2130	Directory Connection source removed	The directory connection source with ID {0} was removed by {1}.
2131	Directory Connection source saved	The {0} directory connection source was saved by {1}.

Manager administrator and policy events (continued) **Table 8-20** 

Code	Summary	Description
2132	Agent Troubleshooting Task	Agent Troubleshooting task of type {0} created by user {1}.
2133	Certificate authority file generated.	Certificate authority file {0} generated.
2134	Certificate authority file is corrupt.	Certificate authority file {0} is corrupt.
2135	Password changed for certificate authority file.	Password changed for certificate authority file {0}. New certificate authority file is {1}.
2136	Server keystore generated.	Server keystore {0} generated for endpoint server {1}.
2137	Server keystore is missing or corrupt.	Server keystore {0} for endpoint server {1} is missing or corrupt.
2138	Server truststore generated.	Server truststore {0} generated for endpoint server {1}.
2139	Server truststore is missing or corrupt.	Server truststore {0} for endpoint server {1} is missing or corrupt.
2140	Client certificates and key generated.	Client certificates and key generated.
2141	Agent installer package generated.	Agent installer package generated for platforms {0}.

Enforce licensing and key ignition events **Table 8-21** 

Code	Summary	Description
2200	End User License Agreement accepted	The Symantec Data Loss Prevention End User License Agreement was accepted by {0}, {1}, {2}.
2201	License is invalid	None
2202	License has expired	One or more of your product licenses has expired. Some system feature may be disabled. Check the status of your licenses on the system settings page.
2203	License about to expire	One or more of your product licenses will expire soon. Check the status of your licenses on the system settings page.
2204	No license	The license does not exist, is expired or invalid. No incidents will be detected.
2205	Keys ignited	The cryptographic keys were ignited by administrator logon.

Enforce licensing and key ignition events (continued) **Table 8-21** 

Code	Summary	Description
2206	Key ignition failed	Failed to ignite the cryptographic keys manually. Please look in the Enforce Server logs for more information. It will be impossible to create new exact data profiles.
2207	Auto key ignition	The cryptographic keys were automatically ignited.
2208	Manual key ignition required	The automatic ignition of the cryptographic keys is not configured. Administrator logon is required to ignite the cryptographic keys. No new exact data profiles can be created until the administrator logs on.

Manager major events events **Table 8-22** 

Code	Summary	Description
2300	Low disk space	Hard disk space is low. Symantec Data Loss Prevention Enforce Server disk usage is over {0}%.
2301	Tablespace is almost full	Oracle tablespace {0} is over {1}% full.
2302	{0} not responding	Detection Server {0} did not update its heartbeat for at least 20 minutes.
2303	Monitor configuration changed	The {0} monitor configuration was changed by {1}.
2304	System update uploaded	A system update was uploaded that affected the following components: {0}.
2305	SMTP server is not reachable.	SMTP server is not reachable. Cannot send out alerts or schedule reports.
2306	Enforce Server started	The Enforce Server was started.
2307	Enforce Server stopped	The Enforce Server was stopped.
2308	Monitor status updater exception	The monitor status updater encountered a general exception. Please look at the Enforce Server logs for more information.
2309	System statistics update failed	Unable to update the Enforce Server disk usage and database usage statistics. Please look at the Enforce Server logs for more information.
2310	Statistics aggregation failure	The statistics summarization task encountered a general exception. Refer to the Enforce Server logs for more information.

Manager major events events (continued) **Table 8-22** 

Code	Summary	Description
2311	Version mismatch	Enforce version is {0}, but this monitor's version is {1}.
2312	Incident deletion failed	Incident Deletion failed .
2313	Incident deletion completed	Incident deletion ran for {0} and deleted {1} incident(s).
2314	Endpoint data deletion failed	Endpoint data deletion failed.
2315	Low disk space on incident server	Hard disk space for the incident data storage server is low. Disk usage is over {0}%.
2316	Over {0} incidents currently contained in the database	Persisting over {0} incidents can decrease database performance.

**Table 8-23** Monitor version support events

Code	Summary	Description
2320	Version obsolete	Detection server is not supported when two major versions older than Enforce server version. Enforce version is {0}, and this detection server"s version is {1}. This detection server must be upgraded.
2321	Version older than Enforce version	Enforce will not have visibility for this detection server and will not be able to send updates to it. Detection server incidents will be received and processed normally. Enforce version is {0}, and this detection server
2322	Version older than Enforce version	Functionality introduced with recent versions of Enforce relevant to this type of detection server will not be supported by this detection server. Enforce version is {0}, and this detection server"s version is {1}.
2323	Minor version older than Enforce minor version	Functionality introduced with recent versions of Enforce relevant to this type of detection server will not be supported by this detection server and might be incompatible with this detection server. Enforce version is {0}, and this detection server"s version is {1}. This detection server should be upgraded.
2324	Version newer than Enforce version	Detection server is not supported when its version is newer than the Enforce server version. Enforce version is {0}, and this detection server"s version is {1}. Enforce must be upgraded or detection server must be downgraded.

Manager reporting events events **Table 8-24** 

Code	Summary	Description
2400	Export web archive finished	Archive "{0}" for user {1} was created successfully.
2401	Export web archive canceled	Archive "{0}" for user {1} was canceled.
2402	Export web archive failed	Failed to create archive "{0}" for user {1}. The report specified had over {2} incidents.
2403	Export web archive failed	Failed to create archive "{0}" for user {1}. Failure occurred at incident {2}.
2404	Unable to run scheduled report	The scheduled report job {0} was invalid and has been removed.
2405	Unable to run scheduled report	The scheduled report {0} owned by {1} encountered an error: {2}.
2406	Report scheduling is disabled	The scheduled report {0} owned by {1} cannot be run because report scheduling is disabled.
2407	Report scheduling is disabled	The scheduled report cannot be run because report scheduling is disabled.
2408	Unable to run scheduled report	Unable to connect to mail server when delivery scheduled report {0}{1}.
2409	Unable to run scheduled report	User {0} is no longer in role {1} which scheduled report {2} belongs to. The schedule has been deleted.
2410	Unable to run scheduled report	Unable to run scheduled report {0} for user {1} because the account is currently locked.
2411	Scheduled report sent	The schedule report {0} owned by {1} was successfully sent.
2412	Export XML report failed	XML Export of report by user [{0}] failed XML Export of report by user [{0}] failed.
2420	Unable to run scheduled data owner report distribution	Unable to distribute report {0} (id={1}) by data owner because sending of report data has been disabled.
2421	Report distribution by data owner failed	Report distribution by data owner for report {0} (id={1}) failed.
2422	Report distribution by data owner finished	Report distribution by data owner for report {0} (id={1}) finished with {2} incidents for {3} data owners. {4} incidents for {5} data owners failed to be exported.

Manager reporting events events (continued) **Table 8-24** 

Code	Summary	Description
2423	Report distribution to data owner truncated	The report distribution {1} (id={2}) for the data owner "{0}" exceeded the maximum allowed size. Only the first {3} incidents were sent to "{0}".
2424	A deprecated version of the Reporting API is being used.	A client is using a deprecated version of the Reporting API that will be disabled with version 13.0 of Data Loss Prevention. Please upgrade the client to v2011 of the API, available with Data Loss Prevention version 11.6 and later, to avoid future service disruptions.

Messaging events **Table 8-25** 

Code	Summary	Description
2500	Unexpected Error Processing Message	{0} encountered an unexpected error processing a message. See the log file for details.
2501	Memory Throttler disabled	{0} x {1} bytes need to be available for memory throttling. Only {2} bytes were available. Memory Throttler has been disabled.

**Table 8-26** Detection server communication events

Code	Summary	Description
2600	Communication error	Unexpected error occurred while sending {1} updates to {0}. {2} Please look at the monitor controller logs for more information.
2650	Communication error(VML)	Unexpected error occurred while sending profile updates config set {0} to {1} {2}. Please look at the monitor controller logs for more information.

**Table 8-27** Monitor controller events

Code	Summary	Description
2700	Monitor Controller started	Monitor Controller service was started.
2701	Monitor Controller stopped	Monitor Controller service was stopped.
2702	Update transferred to {0}	Successfully transferred update package {1} to detection server {0}.

Monitor controller events (continued) **Table 8-27** 

Code	Summary	Description
2703	Update transfer complete	Successfully transferred update package {0} to all detection servers.
2704	Update of {0} failed	Failed to transfer update package to detection server {0}.
2705	Configuration file delivery complete	Successfully transferred config file {0} to detection server.
2706	Log upload request sent.	Successfully sent log upload request {0}.
2707	Unable to send log upload request	Encountered a recoverable error while attempting to deliver log upload request {0}.
2708	Unable to send log upload request	Encountered an unrecoverable error while attempting to deliver log upload request {0}.
2709	Using built-in certificate	Using built-in certificate to secure the communication between Enforce and Detection Servers.
2710	Using user generated certificate	Using user generated certificate to secure the communication between Enforce and Detection Servers.
2711	Time mismatch between Enforce and Monitor. This may affect certain functionalities in the system.	Time mismatch between Enforce and Monitor. It is recommended to fix the time on the monitor through automatic time synchronization.

**Table 8-28** Packet capture events

Code	Summary	Description
2800	Bad spool directory configured for Packet Capture	Packet Capture has been configured with a spool directory: {0}. This directory does not have write privileges. Please check the directory permissions and monitor configuration file. Then restart the monitor.
2801	Failed to send list of NICs. {0}	{0}.

EDM index events and messages **Table 8-29** 

Code	Summary	Description
2900	EDM profile search failed	{0}.
2901	Keys are not ignited	Exact Data Matching will be disabled until the cryptographic keys are ignited.

EDM index events and messages (continued) **Table 8-29** 

Code	Summary	Description
2902	Index folder inaccessible	Failed to list files in the index folder {0}. Check the configuration and the folder permissions.
2903	Created index folder	The local index folder {0} specified in the configuration had not existed. It was created.
2904	Invalid index folder	The index folder {0} specified in the configuration does not exist.
2905	Exact data profile creation failed	Data file for exact data profile "{0}" was not created. Please look in the enforce server logs for more information.
2906	Indexing canceled	Creation of database profile "{0}" was canceled.
2907	Replication canceled	Canceled replication of database profile "{0}" version {1} to server {2}.
2908	Replication failed	Connection to database was lost while replicating database profile {0} to server {1}.
2909	Replication failed	Database error occurred while replicating database profile {0} to server {1}.
2910	Failed to remove index file	Failed to delete index file {1} of database profile {0}.
2911	Failed to remove index files	Failed to delete index files {1} of database profile {0}.
2912	Failed to remove orphaned file	Failed to remove orphaned database profile index file {0}.
2913	Replication failed	Replication of database profile {0} to server {2} failed.{1} Check the monitor controller log for more details.
2914	Replication completed	Completed replication of database profile {0} to server {2}. File {1} was transferred successfully.
2915	Replication completed	Completed replication of database profile {0} to the server {2}. Files {1} were transferred successfully.
2916	Database profile removed	Database profile {0} was removed. File {1} was deleted successfully.
2917	Database profile removed	Database profile {0} was removed. Files {1} were deleted successfully.
2918	Loaded database profile	Loaded database profile {0} from {1}.
2919	Unloaded database profile	Unloaded database profile {0}.

EDM index events and messages (continued) **Table 8-29** 

Code	Summary	Description
2920	Failed to load database profile	{2} No incidents will be detected against database profile "{0}" version {1}.
2921	Failed to unload database profile	{2} It may not be possible to reload the database profile "{0}" version {1} in the future without detection server restart.
2922	Couldn"t find registered content	Registered content with ID {0} wasn"t found in database during indexing.
2923	Database error	Database error occurred during indexing. {0}
2924	Process shutdown during indexing	The process has been shutdown during indexing. Some registered content may have failed to create.
2925	Policy is inaccurate	Policy "{0}" has one or more rules with unsatisfactory detection accuracy against {1}.{2}
2926	Created exact data profile	Created {0} from file "{1}".\nRows processed: {2}\nInvalid rows: {3}\nThe exact data profile will now be replicated to all Symantec Data Loss Prevention Servers.
2927	User Group "{0}" synchronization failed	The following User Group directories have been removed/renamed in the Directory Server and could not be synchronized: {1}.Please update the "{2}" User Group page to reflect such changes.
2928	One or more EDM profiles are out of date and must be reindexed	Check the "Manage > Data Profiles > Exact Data" page for more details. The following EDM profiles are out of date: {0}.

**Table 8-30** IDM index events and messages

Code	Summary	Description
3000	{0}	{1} Document profile wasn't created.
3001	Indexing canceled	Creation of document profile "{0}" was canceled.
3002	Replication canceled	Canceled replication of document profile "{0}" version {1} to server {2}.
3003	Replication failed	Connection to database was lost while replicating document profile "{0}" version {1} to server {2}.
3004	Replication failed	Database error occurred while replicating document profile "{0}" version {1} to server {2}.

IDM index events and messages (continued) **Table 8-30** 

Code	Summary	Description
3005	Failed to remove index file	Failed to delete index file {2} of document profile "{0}" version {1}.
3006	Failed to remove index files	Failed to delete index files {2} of document profile "{0}" version {1}.
3007	Failed to remove orphaned file	{0}
3008	Replication failed	Replication of document profile "{0}" version {1} to server {3} failed. {2}\nCheck the monitor controller log for more details.
3009	Replication completed	Completed replication of document profile "{0}" version {1} to server {3}. File {2} was transferred successfully.
3010	Replication completed	Completed replication of document profile "{0}" version {1} to server {3}.\nFiles {2} were transferred successfully.
3011	Document profile removed	Document profile "{0}" version {1} was removed. File {2} was deleted successfully.
3012	Document profile removed	Document profile "{0}" version {1} was removed. Files {2} were deleted successfully.
3013	Loaded document profile	Loaded document profile "{0}" version {1} from {2}.
3014	Unloaded document profile	Unloaded document profile "{0}" version {1}.
3015	Failed to load document profile	{2}No incidents will be detected against document profile "{0}" version {1}.
3016	Failed to unload document profile	{2} It may not be possible to reload the document profile "{0}" version {1} in the future without monitor restart.
3017	Created document profile	Created "{0}" from "{1}". There are {2} accessible files in the content root. {3} The profile contains index for {4} document(s). {5} The document profile will now be replicated to all Symantec Data Loss Prevention Servers.
3018	Document profile	{0} has reached maximum size. Only {1} out of {2} documents are indexed.
3019	Nothing to index	Document source "{0}" found no files to index.

Attribute lookup events **Table 8-31** 

Code	Summary	Description
3100	Invalid Attributes detected with Script Lookup Plugin	Invalid or unsafe Attributes passed from Standard In were removed during script execution. Please check the logs for more details.
3101	Invalid Attributes detected with Script Lookup Plugin	Invalid or unsafe Attributes passed to Standard Out were removed during script execution. Please check the logs for more details.

**Table 8-32** Monitor stub events

Code	Summary	Description
3200	AggregatorStub started	None
3201	{0} updated	List of updates:{1}.
3202	{0} store intialized	Initial items:{1}.
3203	Received {0}	Size: {1} bytes.
3204	FileReaderStub started	None
3205	IncidentWriterStub started	Using test incidents folder {0}.
3206	Received configuration for {0}	{1}.
3207	PacketCaptureStub started	None
3208	RequestProcessorStub started	None
3209	Received advanced settings	None
3210	Updated settings	Updated settings:{0}.
3211	Loaded advanced settings	None
3212	UpdateServiceStub started	None
3213	DetectionServerDatabaseStub started	None

**Table 8-33** Packet capture events

Code	Summary	Description
3300	Packet Capture started	Packet Capture has successfully started.

Packet capture events (continued) **Table 8-33** 

Code	Summary	Description
3301	Capture failed to start on device {0}	Device {0} is configured for capture, but could not be initialized. Please see PacketCapture.log for more information.
3302	PacketCapture could not elevate its privilege level	PacketCapture could not elevate its privileges. Some initialization tasks are likely to fail. Please check ownership and permissions of the PacketCapture executable.
3303	PacketCapture failed to drop its privilege level	Root privileges are still attainable after attempting to drop them. PacketCapture will not continue
3304	Packet Capture started again as more disk space is available	Packet capture started processing again because some disk space was freed on the monitor hard drives.
3305	Packet Capture stopped due to disk space limit	Packet capture stopped processing packets because there is too little space on the monitor hard drives.
3306	Endace DAG driver is not available	Packet Capture was unable to activate Endace device support. Please see PacketCapture.log for more information.
3307	PF_RING driver is not available	Packet Capture was unable to activate devices using the PF_RING interface. Please check PacketCapture.log and your system logs for more information.
3308	PACKET_MMAP driver is not available	Packet Capture was unable to activate devices using the PACKET_MMAP interface. Please check PacketCapture.log and your system logs for more information.
3309	{0} is not available	Packet Capture was unable to load {0} . No native capture interface is available. Please see PacketCapture.log for more information.
3310	No {0} Traffic Captured	{0} traffic has not been captured in the last {1} seconds. Please check Protocol filters and the traffic sent to the monitoring NIC.
3311	Could not create directory	Could not create directory {0} : {1}.

Log collection events **Table 8-34** 

Code	Summary	Description
3400	Couldn't add files to zip	The files requested for collection could not be written to an archive file.
3401	Couldn't send log collection	The files requested for collection could not be sent.

Log collection events (continued) **Table 8-34** 

Code	Summary	Description
3402	Couldn't read logging properties	A properties file could not be read. Logging configuration changes were not applied.
3403	Couldn't unzip log configuration package	The zip file containing logging configuration changes could not be unpacked. Configuration changes will not be applied.
3404	Couldn't find files to collect	There were no files found for the last log collection request sent to server.
3405	File creation failed	Could not create file to collect endpoint logs.
3406	Disk usage exceeded	File creation failed due to insufficient disk space.
3407	Max open file limit exceeded	File creation failed as max allowed number of files are already open.

Enforce SPC events **Table 8-35** 

Code	Summary	Description
3500	SPC Server successfully registered.	SPC Server successfully registered. Product Instance Id [{0}].
3501	SPC Server successfully unregistered.	SPC Server successfully unregistered. Product Instance Id [{0}].
3502	A self-signed certificate was generated.	A self-signed certificate was generated. Certificate alias [{0}].

**Table 8-36** Enforce user data sources events

Code	Summary	Description
3600	User import completed successfully.	User import from source {0} completed successfully.
3601	User import failed.	User import from data source {0} has failed.
3602	Updated user data linked to incidents.	Updated user data linked to {0} existing incident events.

Catalog item distribution related events events **Table 8-37** 

Code	Summary	Description
3700	Unable to write catalog item	Failed to delete old temporary file {0}.

**Table 8-37** Catalog item distribution related events events (continued)

Code	Summary	Description
3701	Unable to rename catalog item	Failed to rename temporary catalog item file {0}.
3702	Unable to list catalog items	Failed to list catalog item files in folder {0}. Check folder permissions.
3703	Error sending catalog items	Unexpected error occurred while sending an catalog item.{0}Look in the file reader log for more information.
3704	File Reader failed to delete files.	Failed to delete catalog file {0} after it was sent.\nDelete the file manually, correct the problem and restart the File Reader.
3705	Failed to list catalog item files	Failed to list catalog item files in folder {0}. Check folder permissions.
3706	The configuration is not valid.	The property {0} was configured with invalid value {1}. Please make sure that this has correct value provided.
3707	Scan failed: Remediation detection catalog could not be updated	Remediation detection catalog update timed out after {0} seconds for target {1}.

Detection server database events **Table 8-38** 

Code	Summary	Description
3800	DetectionServerDatabase started	None
3801	DetectionServerDatabase failed to start	Error starting DetectionServerDatabase. Reason: {0}.
3802	Invalid Port for DetectionServerDatabase	Could not retrieve the port for DetectionServerDatabase process to listen to connection. Reason: {0}. Check if the property file setting has the valid port number.

Telemetry event code **Table 8-39** 

Code	Summary	Description
3803	Telemetry transmission failed.	Telemetry transmission failed. Transmission status : {0}

Endpoint communication layer events **Table 8-40** 

Code	Summary	Description
3900	Internal communications error.	Internal communications error. Please see {0} for errors. Search for the string {1}.
3901	System events have been suppressed.	System event throttle limit exceeded. {0} events have been suppressed. Internal error code = {1}.

**Table 8-41** Agent communication event code

Code	Summary	Description
4000	Agent Handshaker error	Agent Handshaker error. Please see {0} for errors. Search for the string {1}.

**Table 8-42** Monitor controller replication communication layer application error events

Code	Summary	Description
4050	Agent data batch persist error	Unexpected error occurred while agent data being persisted : {0}. Please look at the monitor controller logs for more information.
4051	Agent status attribute batch persist error	Status attribute data for {0} agent(s) could not be persisted. Please look at the monitor controller logs for more information.
4052	Agent event batch persist	Event data for {0} agent(s) could not be persisted. Please look at the monitor controller logs for more information.

Enforce Server web services event code **Table 8-43** 

Code	Summary	Description
4101	Response Rule Execution Service Database failure on request fetch	Request fetch failed even after {0} retries. Database connection still down. The service will be stopped.

Chapter 9

## Adding a new product module

This chapter includes the following topics:

- Installing a new license file
- About system upgrades

## Installing a new license file

When you first purchase Symantec Data Loss Prevention, upgrade to a later version, or purchase additional product modules, you must install one or more Symantec Data Loss Prevention license files. License files have names in the format <code>name.slf</code>.

You can also enter a license file for one module to start and, later on, enter license files for additional modules.

For detailed information about installing the license file for your initial purchase of Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Installation Guide* for your operating system.

#### To install a license:

- 1 Download the new license file.
  - For information on downloading and extracting a license file, see the document Acquiring Symantec Data Loss Prevention Software, available at the Symantec FileConnect site.
- 2 Go to System > Settings > General and click Configure.
- 3 At the **Edit General Settings** screen, scroll down to the **License** section.

In the Install License field, browse for the new Symantec Data Loss Prevention license file you downloaded, then click Save to agree to the terms and conditions of the end user license agreement (EULA) for the software and to install the license.

Note: If you do not agree to the terms and conditions of the EULA, you cannot install the software.

To enable full functionality of new product license-related features, restart the Vontu Manager Service.

See "About Data Lost Prevention services" on page 76.

The **Current License** list displays the following information for each product license:

- Product The individual Symantec Data Loss Prevention product name
- Count The number of users licensed to use the product
- Status The current state of the product
- **Expiration** The expiration date of license for the product

A month before **Expiration** of the license, warning messages appear on the **System** > Servers > Overview screen. When you see a message about the expiration of your license, contact Symantec to purchase a new license key before the current license expires.

## About system upgrades

The **Upgrade** button on the **System Overview** screen initiates the loading and upgrading of your system to a newer version of Symantec Data Loss Prevention.

For information about upgrading the Symantec Data Loss Prevention software, see the Symantec Data Loss Prevention Upgrade Guide.

See "About Symantec Data Loss Prevention administration" on page 55.

Section 3

## Managing detection servers

- Chapter 10. Installing and managing detection servers
- Chapter 11. Managing log files
- Chapter 12. Using Symantec Data Loss Prevention utilities

# Installing and managing detection servers

#### This chapter includes the following topics:

- About managing Symantec Data Loss Prevention servers
- Enabling Advanced Process Control
- Server controls
- Server configuration—basic
- Server configuration—advanced
- Adding a detection server
- Removing a server
- Importing SSL certificates to Enforce or Discover servers
- About the System Overview screen
- Server status overview
- Recent error and warning events list
- Server Detail screen
- Advanced server settings
- About using load balancers in an endpoint deployment

#### About managing Symantec Data Loss Prevention servers

Symantec Data Loss Prevention servers are managed from the System > Servers > Overview screen. This screen provides an overview of your system, including server status and recent system events. It displays summary information about all Symantec Data Loss Prevention servers, a list of recent error and warning events, and information about your license. From this screen you can add or remove detection servers.

• Click on the name of a server to display its **Server Detail** screen, from which you can control and configure that server.

See "Installing a new license file" on page 173.

See "About the Enforce Server administration console" on page 56.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Adding a detection server" on page 194.

See "Removing a server" on page 196.

See "Server controls" on page 178.

See "Server configuration—basic" on page 180.

## **Enabling Advanced Process Control**

Symantec Data Loss Prevention Advanced Process Control lets you start or stop individual server processes from the Enforce Server administration console. You do not have to start or stop an entire server. This feature can be useful for debugging. When Advanced Process Control is off (the default), each Server Detail screen shows only the status of the entire server. When you turn Advanced Process Control on, the General section of the Server Detail screen displays individual processes.

See "Server Detail screen" on page 201.

#### To enable Advanced Process Control

- Go to System > Settings > General and click Configure.
  - The Edit System Settings screen is displayed.
- 2 Scroll down to the Process Control section and check the Advanced Process Control box.
- 3 Click Save.

Table 10-1 describes the individual processes and the servers on which they run once advanced process control is enabled.

Table 10-1 Advanced processes

Process	Description	Control
Monitor Controller	The Monitor Controller process controls detection servers.	The <b>MonitorController Status</b> is available for the Enforce Server.
File Reader	The File Reader process detects incidents.	The <b>FileReader Status</b> is available for all detection servers.
Incident Writer	The Incident Writer process sends incidents to the Enforce Server.	The IncidentWriter Status is available for all detection servers, unless they are part of a single-tier installation, in which case there is only one Incident Writer process.
Packet Capture	The Packet Capture process captures network streams.	The <b>PacketCapture Status</b> is available for Network Monitor.
Request Processor	The Request Processor processes SMTP requests.	The RequestProcessor Status is available for Network Prevent for Email.
Endpoint Server	The Endpoint Server process interacts with Symantec DLP Agents.	The <b>EndpointServer Status</b> is available for Endpoint Prevent.
Detection Server Database	The Detection Server Database process is used for automated incident remediation tracking.	The <b>DetectionServerDatabase Status</b> is available for Network Discover.

See "Server configuration—basic" on page 180.

#### Server controls

Servers and their processes are controlled from the **Server Detail** screen.

 To reach the Server Detail screen for a particular server, go to the Overview screen (System > Servers > Overview) and click on the server's name in the list.

See "Server Detail screen" on page 201.

The status of the server and its processes appears in the **General** section of the Server Detail screen. The Start, Recycle and Stop buttons control server and process operations.

Current status of the server is displayed in the General section of the Server Detail screen. The possible values are:

Table 10-2 Server status values

Icon	Status
<u>u</u> ,	Starting - In the process of starting.
•	Running - Running without errors.
<u>II</u> )	Running Selected - Some processes on the server are stopped or have errors. To see the statuses of individual processes, you must first enable <b>Advanced Process Control</b> on the <b>System Settings</b> screen.
Ł <sub>II</sub>	Stopping - In the process of stopping.
	Stopped - Fully stopped.
?	Unknown - The Server has encountered one of the following errors:

- Start. To start a server or process, click Start.
- Recycle. To stop and restart a server, click Recycle.
- Stop. To stop a server or process, click **Stop**.
- To halt a process during its start-up procedure, click **Terminate**.

Note: Status and controls for individual server processes are only displayed if Advanced Process Control is enabled for the Enforce Server. To enable Advanced Process Control, go to System > Settings > General > Configure, check the Advanced Process Control box, and click Save.

 To update the status, click the refresh icon in the upper-right portion of the screen, as needed.

See "About Symantec Data Loss Prevention administration" on page 55.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "System events reports" on page 135.

See "Server event detail" on page 139.

#### Server configuration—basic

Enforce Servers are configured from the **System > Settings** menu.

Detection servers are configured from each server's individual Configure Server screen.

#### To configure a server

- Go to the Overview screen (System > Servers > Overview).
- Click on the name of the server in the list.

That server's **Server Detail** screen is displayed. In the upper-left portion of a Server Detail screen are the following buttons:

- Done. Click Done to return to the previous screen.
- Configure. Click Configure to specify a basic configuration for this server.
- Server Settings. Click Server Settings to specify advanced configuration parameters for this server. Use caution when modifying advanced server settings. It is recommended that you check with Symantec Support before changing any of the advanced settings.

See "Server configuration—advanced" on page 193.

See Symantec Data Loss Prevention online Help for information about advanced server configuration.

- Click Configure or Server Settings to display a configuration screen for that type of server.
- Specify or change settings on the screen as needed, and then click **Save**. Click **Cancel** to return to the previous screen without changing any settings.

**Note:** A server must be recycled before new settings take effect.

See "Server controls" on page 178.

The Configure Server screen contains a General section for all detection servers that contains the following parameters:

- Name. The name you choose to give the server. This name appears in the Enforce Server administration console (**System > Servers > Overview**). The name is limited to 255 characters.
- Host. The host name or IP address of the system hosting the server. Host names must be fully qualified. If the host has more than one IP address, specify the address on which the detection server listens for connections to the Enforce Server.
- **Port**. The port number used by the detection server to communicate with the Enforce Server. The default is 8100.

For Single Tier Servers, the **Host** field on the **Configure Server** page is pre-populated with the local IP address 127.0.0.1. You cannot change this value.

The remaining portions of a **Configure Server** screen vary according to the type of server.

See "Network Monitor Server—basic configuration" on page 181.

See "Network Discover Server and Network Protect—basic configuration" on page 190.

See "Network Prevent for Email Server—basic configuration" on page 184.

See "Network Prevent for Web Server—basic configuration" on page 187.

See "Endpoint Server—basic configuration" on page 191.

See "Server Detail screen" on page 201.

See "Classification Server—basic configuration" on page 192.

See "Server Detail screen" on page 201.

### Network Monitor Server—basic configuration

Detection servers are configured from each server's individual Configure Server screen. To display the Configure Server screen, go to the Overview screen (System > Servers > Overview) and click the name of the server in the list. That server's Server Detail screen appears. Click Configure to display the Configure Server screen.

A Network Monitor Server's Configure Server screen is divided into a general section and two tabs:

General section. Use this section to specify the server's name, host, and port.

See "Server configuration—basic" on page 180.

- Packet Capture tab. Use this tab to configure network packet capture settings.
- SMTP Copy Rule tab. Use this tab to modify the source folder where the server retrieves SMTP message files.

The top portion of the **Packet Capture** defines general packet capture parameters. It provides the following fields:

Field	Description
Source Folder Override	The source folder is the directory the server uses to buffer network streams before it processes them. The recommended setting is to leave the <b>Source Folder Override</b> field blank to accept the default. If you want to specify a custom buffer directory, type the full path to the directory.
Archive Folder	If you do not want to archive data, leave the <b>Archive Folder</b> field blank. To archive data, enter the full path to the directory you want to use for that purpose.
Network Interfaces	Select the network interface card(s) to use for monitoring. Note that to monitor a NIC WinPcap software must be installed on the Network Monitor Server.
	See the Symantec Data Loss Prevention Installation Guide for more information about NICs.

Th **Protocol** section of the **Packet Capture** specifies the types of network traffic (by protocol) to capture. It also specifies any custom parameters to apply. This section lists the standard protocols that you have licensed with Symantec, and any custom TCP protocols you have added.

To monitor a particular protocol, check its box. When you initially configure a server, the settings for each selected protocol are inherited from the system-wide protocol settings. You configure these settings by going to System > Settings > Protocol. System-wide default settings are listed as Standard.

Consult Symantec Data Loss Prevention online Help for information about working with system-wide settings.

To override the inherited filtering settings for a protocol, click the name of the protocol. The following custom settings are available (some settings may not be available for some protocols):

- IP filter
- L7 sender filter
- L7 recipient filter
- Content filter
- Search Depth (packets)
- Sampling rate
- Maximum wait until written
- Maximum wait until dropped
- Maximum stream packets
- Minimum stream size
- Maximum stream size
- Segment Interval
- No traffic notification timeout (The maximum value for this setting is 360000 seconds.)

Use the SMTP Copy Rule to modify the source folder where this server retrieves SMTP message files. You can modify the Source Folder by entering the full path to a folder.

See "About Symantec Data Loss Prevention administration" on page 55.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

In addition to the settings available through the Configure Server screen, you can specify advanced settings for this server. To specify advanced configuration parameters, click Server Settings on the server's Overview screen. Use caution when modifying advanced server settings. Check with Symantec Support before you change any advanced setting.

See "Advanced server settings" on page 203.

See the Symantec Data Loss Prevention online Help for information about advanced server settings.

## Network Prevent for Email Server—basic configuration

Detection servers are configured from each server's individual Configure Server screen. To display the **Configure Server** screen, go to the **Overview** screen (System > Servers > Overview) and click the name of the server in the list. That server's Server Detail screen appears. Click Configure to display the Configure Server screen.

A Network Prevent for Email Server Configure Server screen is divided into a General section and an Inline SMTP tab. The General section specifies the server's name, host, and port.

See "Server configuration—basic" on page 180.

Use the Inline SMTP tab to configure different Network Prevent for Email Server features:

Field	Description
Trial Mode	Trial mode lets you test prevention capabilities without blocking requests. When trial mode is selected, the server detects incidents and creates incident reports, but does not block any messages. Deselect this option to block those messages that are found to violate Symantec Data Loss Prevention policies.
Keystore Password	If you use TLS authentication in a forwarding mode configuration, enter the correct password for the keystore file.
Next Hop Configuration	Select <b>Reflect</b> to operate Network Prevent for Email Server in reflecting mode. Select <b>Forward</b> to operate in forwarding mode.
	<b>Note:</b> If you select <b>Forward</b> you must also select <b>Enable MX Lookup</b> or <b>Disable MX Lookup</b> to configure the method that is used to determine the next-hop MTA.

Field

**Enable MX Lookup** 

### Description

This option applies only to forwarding mode configurations.

Select **Enable MX Lookup** to perform a DNS query on a domain name to obtain the mail exchange (MX) records for the server. Network Prevent for Email Server uses the returned MX records to select the address of the next hop mail server.

If you select Enable MX Lookup, also add one or more domain names in the Enter **Domains** text box. For example:

companyname.com

Network Prevent for Email Server performs MX record queries for the domain names that you specify.

Note: You must include at least one valid entry in the Enter Domains text box to successfully configure forwarding mode behavior.

#### Field

#### Disable MX Lookup

#### Description

This field applies only to forwarding mode configurations.

Select **Disable MX Lookup** if you want to specify the exact or IP address of one or more next-hop MTAs. Network Prevent for Email Server uses the hostnames or addresses that you specify and does not perform an MX record lookup.

If you select **Disable MX Lookup**, also add one or more hostnames or IP addresses for next-hop MTAs in the Enter Hostnames text box. You can specify multiple entries by placing each entry on a separate line. For example:

```
smtp1.companyname.com
smtp2.companyname.com
smtp3.companyname.com
```

Network Prevent for Email Server always tries to use the first MTA that you specify in the list. If that MTA is not available. Network Prevent for Email Server tries the next available entry in the list.

**Note:** You must include at least one valid entry in the Enter Hostnames text box to successfully configure forwarding mode behavior.

See the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent for Email for additional information about configuring Network Prevent for Email Server options.

See "About Symantec Data Loss Prevention administration" on page 55.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

In addition to the settings available through the Configure Server screen, you can specify advanced settings for this server. To specify advanced configuration parameters, click Server Settings on the server's Overview screen. Use caution

when modifying advanced server settings. Check with Symantec Support before you change any advanced setting.

See "Advanced server settings" on page 203.

See the Symantec Data Loss Prevention online Help for information about advanced server settings.

### Network Prevent for Web Server—basic configuration

Detection servers are configured from each server's individual Configure Server screen. To display the Configure Server screen, go to the Overview screen (System > Servers > Overview) and click the name of the server in the list. That server's Server Detail screen appears. Click Configure to display the Configure Server screen.

A Network Prevent for Web Server Configure Server screen is divided into a general section and one tab:

- **General** section. This section specifies the server's name, host, and port. See "Server configuration—basic" on page 180.
- ICAP tab. This tab is for configuring Internet Content Adaptation Protocol (ICAP) capture.

Use the ICAP tab to configure Web-based network traffic. The ICAP tab is divided into four sections:

- The **Trial Mode** section enables you to test prevention without blocking traffic. When trial mode is selected, the server detects incidents and creates incident reports, but it does not block any traffic. This option enables you to test your policies without blocking traffic. Check the box to enable trial mode.
- The Request Filtering section configures traffic filtering criteria:

Field	Description
Ignore Requests Smaller Than	Specify the minimum body size of HTTP requests to inspect on this server. The default value is 4096 bytes. HTTP requests with bodies smaller than this number are not inspected.
Ignore Requests without Attachments	Check this box to inspect only those HTTP requests that contain attachments.

Field	Description
Ignore Requests to Hosts or Domains	Enter the host names or domains whose requests should be filtered out (ignored). Enter one host or domain name per line.
Ignore Requests from User Agents	Enter the names of user agents whose requests should be filtered out (ignored). Enter one agent per line.

The **Response Filtering** section configures the filtering criteria to manage HTTP responses:

Field	Description
Ignore Responses Smaller Than	Enter the minimum body size of HTTP responses to inspect on this server. The default value is 4096 bytes. HTTP responses with bodies smaller than this number are not inspected.
Inspect Content Type	Specify the MIME content types that this server is to monitor. By default, this field contains content type values for standard Microsoft Office, PDF, and plain-text formats. You can add other MIME content type values. Enter separate content types on separate lines. For example, to inspect WordPerfect 5.1 files, enter application/wordperfect5.1.
Ignore Responses from Hosts or Domains	Enter the host names or domains whose responses are to be ignored. Enter one host or domain name per line.

Description

Field	Description
Ignore Responses to User Agents	Enter the names of user agents whose responses are to be ignored. Enter one user agent per line.

■ The Connection section configures settings for the ICAP connection between an HTTP proxy server and the Network Prevent for Web Server:

rieiu	Description
TCP Port	Specify the TCP port number that this server is to use to listen to ICAP requests. The same value must be configured on the HTTP proxy sending ICAP requests to this server. The recommended value is 1344.
Maximum Number of Requests	Enter the maximum number of simultaneous ICAP request connections. The default is 25.
Maximum Number of Responses	Enter the maximum number of simultaneous ICAP response connections from the HTTP proxy or proxies that are allowed. The default is 25.
Connection Backlog	Enter the maximum number of waiting connections allowed. Each waiting connection means that a user waits at their browser. The minimum value is 1.

See "Configuring Network Prevent for Web Server" on page 1167.

See "About Symantec Data Loss Prevention administration" on page 55.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

Field

In addition to the settings available through the Configure Server screen, you can specify advanced settings for this server. To specify advanced configuration parameters, click Server Settings on the server's Overview screen. Use caution when modifying advanced server settings. Check with Symantec Support before you change any advanced setting.

See "Advanced server settings" on page 203.

See the Symantec Data Loss Prevention online Help for information about advanced server settings.

### Network Discover Server and Network Protect—basic configuration

Detection servers are configured from each server's individual Configure Server screen. To display the Configure screen for a server, go to the Overview screen (System > Servers > Overview) and click on the name of the server in the list. That server's **Server Detail** screen is displayed. Click **Configure**. The server's Configure Server screen is displayed.

See "Modifying the Network Discover Server configuration" on page 1185.

A Network Discover Server's **Configure Server** screen is divided into a general section and one tab:

- General section. This section is for specifying the server's name, host, and port. See "Server configuration—basic" on page 180.
- Discover tab. This tab is for modifying the number of parallel scans that run on this Discover Server.

The maximum count can be increased at any time. After it is increased, any queued scans that are eligible to run on the Network Discover Server are started. The count can be decreased only if the Network Discover Server has no running scans. Before you reduce the count, pause, or stop, all scans running on the

To view the scans running on Network Discover Servers, go to Manage > **Discover Scanning > Discover Targets.** 

See "About Symantec Data Loss Prevention administration" on page 55.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

In addition to the settings available through the Configure Server screen, you can also specify advanced settings for this server. To specify advanced configuration parameters, click Server Settings on the Server Detail screen. Use caution when modifying advanced server settings. It is recommended that you check with Symantec Support before changing any of the advanced settings.

See "Advanced server settings" on page 203.

### Endpoint Server—basic configuration

Detection servers are configured from each server's individual Configure Server screen. To display the Configure screen for a server, go to the Overview screen (System > Servers > Overview) and click the name of the server. The Server Detail screen for that server is displayed. Click Configure to display the Configure Server screen for that server.

See "Adding a detection server" on page 194.

The **Configure Server** screen for an Endpoint Server is divided into a general section and the following tabs:

- General. This section is for specifying the server name, host, and port. See "Server configuration—basic" on page 180.
- Agent. This section is for adding agent security certificates to the Endpoint Server.

See "Adding agent configurations" on page 1406.

**Agent Listener**. Use this section to configure the Endpoint Server to listen for connections from Symantec DLP Agents:

Field	Description
Bind address	Enter the IP address on which the Endpoint Server listens for communications from the Symantec DLP Agents. The default IP address is 0.0.0.0 which allows the Endpoint Server to listen on all host IP addresses.
Port	Enter the port over which the Endpoint Server listens for communications from the Symantec DLP Agents.

See "Configuring Endpoint Servers for SSL certificates" on page 191.

### **Configuring Endpoint Servers for SSL certificates**

Table 10-3 provides steps for loading SSL certificates into an Endpoint Server.

Note: These steps assume that you have generated the endpoint certificates and that the server \*.jks files are available to the Enforce Server.

	Table 10-3	Instructions for loading SSL certificates into an Endpoint Server
Step	Action	Description
1	Go to the System > Servers > Overview screen.	The screen is available to administrative users in the Enforce Server administration console.
2	Select the <b>Endpoint Server</b> you want to configure.	Each Endpoint Server must be configured for SSL communications separately.
3	Click Configure.	An Endpoint Server cannot communicate with DLP Agents until it is configured with SSL certificates.
4	Select the <b>Agent</b> tab.	The Agent tab provides the interface for passing certificates to the Endpoint Server.
5	Specify the <b>Security Configuration</b> for the Endpoint Server.	Load the SSL certificates as follows:  Keystore File: Browse to and select the file eps_keystore.jks, which is the CA-signed private key for the Endpoint Server.  Keystore Password: enter the password for the keystore.  Truststore File: Browse to and select the file eps_truststore.jks, which is the public key for DLP Agents connecting to this Endpoint Server.  Truststore Password: enter the truststore password.
6	Click Save.	If you get an error message, you need to make sure you generated the certificates properly and added the files and passwords properly.
7	Restart the Endpoint Server.	Navigate to the System > Servers > Overview > Server Detail screen.  Click Recycle.
8	Click <b>Done</b> when the server has restarted.	Verify that the server restarts.

### Classification Server—basic configuration

Install DLP Agents.

9

Detection servers are configured from each server's individual Configure Server screen. To display the **Configure Server** screen, go to the **Overview** screen (System > Servers > Overview) and click the name of the server in the list. The Server Detail screen for that server appears. Click Configure to display the Configure Server screen.

The **Configure Server** screen for a Classification Server is divided into two sections:

- **General** section. This section specifies the server name, host, and port that is used for communicating with the Enforce Server. See "Server configuration—basic" on page 180.
- Classification section. This section specifies the connection properties that the Data Classification for Enterprise Vault filter uses to communicate with the Classification Server.

Use the fields of the Classification section to configure connection properties for the server:

Maximum number of sessions	Enter the maximum number of concurrent

sessions that the Classification Server can accept from Data Classification for Enterprise Vault filters. The default is 12. The maximum number of sessions that a Classification Server can support depends on the CPU and memory available to the server. See the Symantec Enterprise Vault Data Classification Services Implementation Guide for more information

Session Timeout (in milliseconds) Enter the maximum number of milliseconds

that a Data Classification for Enterprise Vault filter can remain idle before the Classification Server terminates the session. The default

value is 30000 milliseconds

Classification Service Port Specify the port number on which the

> Classification Server accepts connections from Data Classification for Enterprise Vault

filters. The default port is 10080.

Note: The Classification Server is used only with the Symantec Enterprise Vault Data Classification solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Enterprise Vault Data Classification Services filter and Classification Server to communicate with one another. See the Symantec Enterprise Vault Data Classification Services Implementation Guide for more information.

## Server configuration—advanced

Symantec Data Loss Prevention provides advanced server configuration settings for each detection server in your system.

Note: Check with Symantec Support before changing any advanced settings. If you make a mistake when changing advanced settings, you can severely degrade performance or even disable the server entirely.

### To change an advanced configuration setting for a detection server

Go to **System > Servers > Overview** and click on the name of the detection server.

That server's **Server Detail** screen appears.

Click Server Settings.

The Advanced Server Settings screen appears.

See Symantec Data Loss Prevention online Help for information about advanced server configuration.

See "Advanced server settings" on page 203.

- With the guidance of Symantec Support, modify the appropriate setting(s).
- Click Save.

Changes to settings on this screen normally do not take effect until you restart the server.

See "Server configuration—basic" on page 180.

## Adding a detection server

Add the detection servers that you want to your Symantec Data Loss Prevention system from the **System > Servers > Overview** screen.

You can add the following types of servers:

- Network Monitor Server, which monitors network traffic.
- Network Discover Server, which inspects stored data for policy violations.
- Network Prevent for Email Server, which prevents SMTP violations.
- Network Prevent for Web Server, which prevents ICAP proxy server violations such as FTP, HTTP, and HTTPS.
- Mobile Prevent for Web Server, which monitors and prevents HTTPS, HTTPS, and FTP violations over mobile devices using a VPN.
- Endpoint Prevent, which controls Symantec DLP Agents that monitor and scan endpoints.

- Classification Server, which analyzes emails sent from a Symantec Enterprise Vault filter and provides a classification result that Enterprise Vault can use to perform tagging, archival, and deletion as necessary
- Mobile Email Monitor Server, which monitors corporate emails sent through Microsoft Exchange ActiveSync and downloaded to mobile devices.
- Single-Tier Server: By selecting the Single-Tier Server option, the detection servers that you have licensed are installed on the same host as the Enforce Server. The single-tier server performs detection for the following products (you must have a license for each): Network Monitor, Network Discover, Network Prevent for Email, Network Prevent for Web, and Endpoint Prevent.

#### To add a detection server

- Go to the **System Overview** screen (**System > Servers > Overview**). See "About the System Overview screen" on page 198.
- 2 Click Add Server.

The **Add Server** screen appears.

3 Select the type of server you want to install and click **Next**.

The **Configure Server** screen for that detection server appears.

4 To perform the basic server configuration, use the **Configure Server** screen, then click Save when you are finished.

See "Network Monitor Server—basic configuration" on page 181.

See "Network Prevent for Email Server—basic configuration" on page 184.

See "Network Prevent for Web Server—basic configuration" on page 187.

See "Network Discover Server and Network Protect—basic configuration" on page 190.

See "Adding and configuring the Mobile Email Monitor Server" on page 1560.

See "Endpoint Server—basic configuration" on page 191.

See "Classification Server—basic configuration" on page 192.

For Single-Tier Servers, the **Configure Server** page displays a configuration tab for each of your licensed detection servers. See the basic configuration topics for each detection type you want to configure.

5 To return to the **System Overview** screen, click **Done**.

Your new server is displayed in the **Servers** list with a status of **Unknown**.

Click on the server to display its **Server Detail** screen. 6

See "Server Detail screen" on page 201.

- 7 Click [Recycle] to restart the server.
- 8 Click **Done** to return to the **System Overview** screen.

When the server is finished restarting, its status displays **Running**.

If necessary, click Server Settings on the Server Detail screen to perform Advanced Server configuration.

See "Advanced server settings" on page 203.

See Symantec Data Loss Prevention online Help for information about Advanced Server configuration.

See "Server configuration—basic" on page 180.

## Removing a server

See the appropriate Symantec Data Loss Prevention Installation Guide for information about uninstalling Symantec Data Loss Prevention from a server.

An Enforce Server administration console lists the detection servers registered with it on the **System > Overview** screen. If Symantec Data Loss Prevention is uninstalled from a detection server, or that server is stopped or disconnected from the network, its status is shown as Unknown on the console.

A detection server can be removed (de-registered) from an Enforce Server administration console. When a detection server is removed from an Enforce Server. its Symantec Data Loss Prevention services continue to operate. This means that even though a detection server is de-registered from Enforce, it continues to function unless some action is taken to halt it. In other words, even though it is removed from an Enforce Server administration console, a detection server continues to operate. Incidents it detects are stored on the detection server. If a detection server is re-registered with an Enforce Server, incidents detected and stored are then forwarded to Enforce.

#### To remove (de-register) a detection server from Enforce

Go to System > Overview.

See "About the System Overview screen" on page 198.

In the **Servers** section of the screen, click the red X on a server's status line to remove it from this Enforce Server administration console.

See "Server controls" on page 178.

3 Click **OK** to confirm.

The server's status line is removed from the System Overview list.

## Importing SSL certificates to Enforce or Discover servers

You can import SSL certificates to the Java trusted keystore on the Enforce or Discover servers. The SSL certificate can be self-signed (server) or issued by a well-known certificate authority (CA).

You may need to import an SSL certificate to make secure connections to external servers such as Active Directory (AD). If a recognized authority has signed the certificate of the external server, the certificate is automatically added to the Enforce Server. If the server certificate is self-signed, you must manually import it to the the Enforce or Discover Servers.

Importing an SSL certificate to Enforce or Discover **Table 10-4** 

Step	Description
1	Copy the certificate file you want to import to the Enforce Server or Discover Server computer.
2	Change directory to c:\SymantecDLP\jre\bin on the Enforce Server or Discover Server computer.
3	Execute the keytool utility with the -importcert option to import the public key certificate to the Enforce Server or Discover Server keystore:
	<pre>keytool -importcert -alias new_endpointgroup_alias -keystore\lib\security\cacerts -file my-domaincontroller.crt</pre>
	In this example command, <code>new_endpointgroup_alias</code> is a new alias to assign to the imported certificate and <code>my-domaincontroler.crt</code> is the path to your certificate.
4	When you are prompted, enter the password for the keystore.
	By default, the password is <b>changeit</b> . If you want you can change the password when prompted.
	To change the password, use: keytool -storepassword -alias
	<pre>new_endpointgroup_alias -keystore\lib\security\cacerts</pre>
5	Answer <b>Yes</b> when you are asked if you trust this certificate.
6	Restart the Enforce Server or Discover Server.

See "Configuring directory server connections" on page 127.

## About the System Overview screen

The System Overview screen is reached by System > Servers > Overview. This screen provides a guick snapshot of system status. It lists information about the Enforce Server, and each registered detection server.

The **System Overview** screen provides the following features:

- The **Add Server** button is used to register a detection server. When this screen is first viewed after installation, only the Enforce Server is listed. You must register your various detection servers with the Add Server button. After you register detection servers, they are listed in the **Servers** section of the screen. See "Adding a detection server" on page 194.
- The **Upgrade button** is for upgrading Symantec Data Loss Prevention to a newer version.
  - See "About system upgrades" on page 174.
  - See also the appropriate Symantec Data Loss Prevention Upgrade Guide.
- The **Servers** section of the screen displays summary information about each server's status. It can also be use to remove (de-register) a server. See "Server status overview" on page 198.
- The Recent Error and Warning Events section shows the last five events of error or warning severity for any of the servers listed in the Servers section. See "Recent error and warning events list" on page 200.
- The **License** section of the screen lists the Symantec Data Loss Prevention individual products that you are licensed to use.

See "Server configuration—basic" on page 180.

See "About Symantec Data Loss Prevention administration" on page 55.

### Server status overview

The Server section of the System Overview screen is reached by System > Servers > Overview. This section of the screen provides a quick overview of system status.

**Table 10-5** Server statuses

Icon	Status	Description
<u>II</u> )	Starting	The server is starting up.

Server statuses (continued) Table 10-5

Icon	Status	Description
•	Running	The server is running normally without errors.
Щ.	Running Selected	Some Symantec Data Loss Prevention processes on the server are stopped or have errors. To see the statuses of individual processes, you must first enable <b>Advanced Process Control</b> on the <b>System Settings</b> screen.  See "Enabling Advanced Process Control" on page 177.
		Oce Enabling Advanced Process Control on page 177.
<b>Ľ</b> ∥	Stopping	The server is in the process of stopping Symantec Data Loss Prevention services.  See "About Data Lost Prevention services" on page 76.
	Stopped	All Symantec Data Loss Prevention processes are stopped.
?	Unknown	<ul> <li>The server is experiencing one of the following errors:</li> <li>The Enforce Server is not reachable from server.</li> <li>Symantec Data Loss Prevention is not installed on the server.</li> <li>A license key has not been configured for the Enforce Server.</li> <li>There is problem with Symantec Data Loss Prevention account permissions in Windows.</li> </ul>

For each server, the following additional information appears. You can also click on any server name to display the **Server Detail** screen for that server.

Table 10-6 Server status additional information

Column name	Description
Messages (Last 10 sec)	The number of messages processed in the last 10 seconds
Messages (Today)	The number of messages processed since 12 am today
Incidents (Today)	The number of incidents processed since 12 am today For Endpoint Servers, the Messages and Incidents are not aligned. This is because messages are being processed at the Endpoint and not the Endpoint Server. However, the incident count still increases.

Table 10 0 Server status additional information (continued)		
Column name	Description	
Incident Queue	For the Enforce Server, this is the number of incidents that are in the database, but do not yet have an assigned status. This number is updated whenever this screen is generated.	
	For the other types of servers, this is the number of incidents that have not yet been written to the Enforce Server. This number is updated approximately every 30 seconds. If the server is shut down, this number is the last number updated by the server. Presumably the incidents are still in the incidents folder.	
Message Wait Time	The amount of time it takes to process a message after it enters the system. This data applies to the last message processed. If the server that processed the last message is disconnected, this is N/A.	

**Table 10-6** Server status additional information (continued)

#### To see details about a server

Click on any server name to see additional details regarding that server.

See "Server Detail screen" on page 201.

#### To remove a server from an Enforce Server

Click the red X for that server, and then confirm your decision.

Note: Removing (de-registering) a server only disconnects it from this Enforce Server server, it does not stop the detection server from operating.

See "Removing a server" on page 196.

## Recent error and warning events list

The Recent Error and Warning Events section of the System Overview screen is reached by Systern > Servers > Overview. This section of the screen shows the last five events of either error or warning severity for any of the servers listed in the Servers section.

Column name	Description
Туре	<u>^</u>
	⊗
	The yellow triangle indicates a warning, the red circle indicates an error.
Time	The date and time when the event occurred.
Server	The name of the server on which the event occurred.
Host	The IP address or name of the machine where the server resides. The server and host names may be the same.
Code	The system event code. The <b>Message</b> column provides the code text. Event lists can be filtered by code number.
Message	A summary of the error or warning message that is associated with this event code.

Recent error and warning events information **Table 10-7** 

- To display a list of all error and warning events, click **Show all**.
- To display the Event Detail screen for additional information about that particular event, click an event.

See "About the System Overview screen" on page 198.

See "System events reports" on page 135.

See "Server event detail" on page 139.

## Server Detail screen

The Server Detail screen (located by clicking an Endpoint Server on the System > Servers > Overview screen) provides detailed information about a single selected server. The **Server Detail** screen is also used to control and configure a server.

To display the Server Detail screen for a particular server

- 1 Navigate to the **System > Servers > Overview** screen.
- 2 Click the detection server name in the **Server Overview** list.

See "About the System Overview screen" on page 198.

The Server Detail screen is divided into sections. The sections listed below display all server types. The system displays sections based on the type of detection server.

Server Detail screen display information **Table 10-8** 

Server Detail display sections	Description	
General	The <b>General</b> section identifies the server, displays system status and statistics, and provides controls for starting and stopping the server and its processes.	
	See "Server controls" on page 178.	
Configuration	The <b>Configuration</b> section displays the Channels, Policy Groups, Agent Cofiguration, User Device, and Cofiguration Status for the detection server.	
All Agents	The <b>All Agents</b> section displays a summary of all agents that are assigned to the Endpoint Server. Current agents display in the <b>12.5</b> and Later column and older agents display in the <b>12.0.x</b> and Earlier column	
	Click the number next to an agent status to view agent details on the System > Agents > Overview > Summary Reports screen.	
	<b>Note:</b> The system only displays the <b>Agent Summary</b> section for an Endpoint Server.	
Recent Error and Warning Events	The <b>Recent Error and Warning Events</b> section displays the five most recent Warning or Severe events that have occurred on this server.	
	Click on an event to show event details. Click <b>show all</b> to display all error and warning events.	
	See "About system events" on page 134.	
All Recent Events	The <b>All Recent Events</b> section displays all events of all severities that have occurred on this server during the past 24 hours.	
	Click on an event to show event details. Click <b>show all</b> to display all detection server events.	
Deployed Data Profiles	The Deployed Data Profile section lists any <b>Exact Data</b> or <b>Document Profiles</b> you have deployed to the detection server. The system displays the version of the index in the profile.	
	See "Data Profiles" on page 291.	

See "About the System Overview screen" on page 198.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

See "System events reports" on page 135.

See "Server event detail" on page 139.

# **Advanced server settings**

Use the Server Settings tab of a detection server's System > Servers > Overview > Server Detail screen to modify the settings on that server.

Use caution when modifying these settings on a server. Contact Symantec Support before changing any of the settings on this screen. Changes to these settings normally do not take effect until after the server has been restarted.

You cannot change settings for the Enforce Server from the Server Detail screen. The **Server Settings** tab only displays for detection servers.

Note: If you change advanced server settings to Endpoint Servers in a load-balanced environment, you must apply the same changes to all Endpoint Servers in the load-balanced environment.

Detection server advanced settings **Table 10-9** 

Setting	Default	Description
BoxMonitor.Channels	Varies	The values are case-sensitive and comma-separated if multiple.
		Although any mix of them can be configured, the following are the officially supported configurations:
		<ul> <li>Network Monitor Server: Packet Capture, Copy Rule</li> <li>Discover Server: Discover</li> <li>Endpoint Server: Endpoint</li> <li>Network Prevent for Email: Inline SMTP</li> <li>Network Prevent for Web: ICAP</li> <li>Mobile Email Monitor: ICAP</li> <li>Classification Server: Classification</li> </ul>

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
BoxMonitor.DetectionServerDatabase	on	Enables the BoxMonitor process to start the Automated Incident Remediation Tracking database on the Detection Server. If you set this to off, you must start the remediation tracking database manually.
BoxMonitor.DetectionServerDatabaseMemory	-Xrs -Xms300M -Xmx1024M	Any combination of JVM memory flags can be used.
BoxMonitor.DiskUsageError	90	The amount of disk space filled (as a percentage) that will trigger a severe system event. For instance, if Symantec Data Loss Prevention is installed on the C drive and this value is 90, then the detection server creates a severe system event when the C drive usage is above 90%.
BoxMonitor.DiskUsageWarning	80	The amount of disk space filled (as a percentage) that will trigger a warning system event. For instance, if Symantec Data Loss Prevention is installed on the C drive and this value is <b>80</b> , then the detection server generates a warning system event when the C drive usage is above 80%.
BoxMonitor.EndpointServer	on	Enables the Endpoint Server.
BoxMonitor.EndpointServerMemory		Any combination of JVM memory flags can be used. For example: -Xrs -Xms300m -Xmx1024m.
BoxMonitor.FileReader	on	If off, the BoxMonitor cannot start the FileReader, although it can still be started manually.
BoxMonitor.FileReaderMemory	-Xrs -Xms1200M -Xmx3200M -XX:PermSize=128M -XX:MaxPermSize	FileReader JVM command-line arguments.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
BoxMonitor.HeartbeatGapBeforeRestart	960000	The time interval (in milliseconds) that the BoxMonitor waits for a monitor process (for example, FileReader, IncidentWriter) to report the heartbeat. If the heartbeat is not received within this time interval the BoxMonitor restarts the process.
BoxMonitor.IncidentWriter	on	If off, the BoxMonitor cannot start the IncidentWriter in the two-tier mode, although it can still be started manually. This setting has no effect in the single-tier mode.
BoxMonitor.IncidentWriterMemory		IncidentWriter JVM command-line arguments. For example: <b>-Xrs</b>
BoxMonitor.InitialRestartWaitTime	5000	
BoxMonitor.MaxRestartCount	3	
BoxMonitor.MaxRestartCountDuringStartup	5	The maximum times that the monitor server will attempt to restart on its own.
BoxMonitor.PacketCapture	on	If off, the BoxMonitor cannot start PacketCapture, although it can still be started manually. The PacketCapture channel must be enabled for this setting to work.
BoxMonitor.PacketCaptureDirectives		PacketCapture command line parameters (in Java). For example: -Xrs
BoxMonitor.ProcessLaunchTimeout	30000	The time interval (in milliseconds) for a monitor process (e.g. FileReader) to start.
BoxMonitor.ProcessShutdownTimeout	45000	The time interval (in milliseconds) allotted to each monitor process to shut down gracefully. If the process is still running after this time the BoxMonitor attempts to kill the process.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
BoxMonitor.RequestProcessor	on	If off, the BoxMonitor cannot start the RequestProcessor; although, it can still be started manually. The Inline SMTP channel must be enabled for this setting to work.
BoxMonitor.RequestProcessorMemory		Any combination of JVM memory flags can be used. For example: -Xrs -Xms300M -Xmx1300M
BoxMonitor.RmiConnectionTimeout	15000	The time interval (in milliseconds) allowed to establish connection to the RMI object.
BoxMonitor.RmiRegistryPort	37329	The TCP port on which the BoxMonitor starts the RMI registry.
BoxMonitor.StatisticsUpdatePeriod	10000	The monitor statistics are updated after this time interval (in milliseconds).
Classification.BindAddress	0.0.0.0	The IP address on which the Classification Server accepts messages for detection. By default, the Classification Server listens on all interfaces (0.0.0.0). If you have a multi-homed server computer and you want to limit classification requests to a specific network interface, enter the IP address of that interface in this field.
Classification.MaxMemory	120M	The maximum amount of memory that the Classification Server allocates. After this limit is reached, any additional requests to classify Exchange messages are spooled to disk until memory is freed.
Classification.SessionReapInterval	20000	The time interval (in milliseconds) after which the Classification Server purges stale sessions.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Classification.WebserviceLogRententionDays	7	The number of days to retain the Classification Server web service request log. These log files are stored in c:\SymantecDLP\Protect\logs\jetty (Windows) or /var/log/SymantecDLP/logs/jetty (Linux).
ContentExtraction.EnableMetaData	off	Allows detection on file metadata. If the setting is turned on, you can detect metadata for Microsoft Office and PDF files. For Microsoft Office files, OLE metadata is supported, which includes the fields Title, Subject, Author, and Keywords. For PDF files, only Document Information Dictionary metadata is supported, which includes fields such as Author, Title, Subject, Creation, and Update dates. Extensible Metadata Platform (XMP) content is not detected. Note that enabling this metadata detection option can cause false positives.
ContentExtraction.LongContentSize	1M	If the message component exceeds this size (in bytes) then the ContentExtraction.LongTimeout is used instead of ContentExtraction.ShortTimeout.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
ContentExtraction.LongTimeout	Varies	The default value for this setting varies depending on detection server type (60,000 or 120,000).
		The time interval (in milliseconds) given to the ContentExtractor to process a document larger than ContentExtraction.LongContentSize. If the document cannot be processed within the specified time it's reported as unprocessed. This value should be greater than ContentExtraction.ShortTimeout and less than ContentExtraction.RunawayTimeout.
ContentExtraction.MarkupAsText	off	Bypasses Content Extraction for files that are determined to be XML or HTML. This should be used in cases such as web pages containing data in the header block or script blocks. Default is off.
ContentExtraction.MaxContentSize	30M	The maximum size (in MB) of the document that can be processed by the ContentExtractor.
ContentExtraction.RunawayTimeout	300,000	The time interval (in milliseconds) given to the ContentExtractor to finish processing of any document. If the ContentExtractor does not finish processing some document within this time it will be considered unstable and it will be restarted. This value should be significantly greater than ContentExtraction.LongTimeout.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
ContentExtraction.ShortTimeout	30,000	The time interval (in milliseconds) given to the ContentExtractor to process a document smaller than ContentExtraction.LongContentSize. If the document cannot be processed within the specified time it is reported as unprocessed. This value should be less than ContentExtraction.LongTimeout.
ContentExtraction.TrackedChanges	off	Allows detection of content that has changed over time (Track Changes content) in Microsoft Office documents.
		<b>Note:</b> Using the foregoing option might reduce the accuracy rate for IDM and data identifiers. The default is set to off (disallow).
		To index content that has changed over time, set
		ContentExtraction.TrackedChanges=on in file
		\Protect\config\Indexer.properties. The default and recommended setting is
		ContentExtraction.TrackedChanges=off.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
DDM.MaxBinMatchSize	300,000,000	The maximum size (in bytes) used to generate the MD5 hash for an exact binary match in an IDM. This setting should not be changed. The following conditions must be matched for IDM to work correctly:  This setting must be exactly identical to the max_bin_match_size setting on the Enforce Server in file indexer.properties.  This setting must be smaller or equal to the FileReader.FileMaxSize value.  This setting must be smaller or equal to the ContentExtraction.MaxContentSize value on the Enforce Server in file indexer.properties.  Note: Changing the first or third item in the list requires re-indexing all IDM files.
DDM.UseJavaMD5	false	Setting this flag to <b>true</b> makes the indexer/detection use the default Java MD5. False uses a faster MD5 library. In general, this setting should not be changed. If it is it must match the setting in the Indexer.properties file.
Detection.EncodingGuessingDefaultEncoding	ISO-8859-1	Specifies the backup encoding assumed for a byte stream.
Detection.EncodingGuessingEnabled	on	Designates whether the encoding of unknown byte streams should be guessed.
Detection.EncodingGuessingMinimumConfidence	50	Specifies the confidence level required for guessing the encoding of unknown byte streams.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Detection.MessageTimeout ReportIntervalInSeconds	3600	Number of seconds between each System Event published to display the number of messages that have timed out recently. These System Events are scheduled to be published at a fixed rate, but will be skipped if no messages have timed out in that period.
DI.MaxViolations	100	Specifies the maximum number of violations allowed with data identifiers.
Discover.CountAllFilteredItems	false	Provides more accurate scan statistics by counting the items in folders skipped because of filtering. To count all items, set this setting to true.
Discover.Exchange.FollowRedirects	true	Specifies whether to follow redirects. Symantec Data Loss Prevention follows redirects only from the public root folder.
Discover.Exchange.ScanHiddenItems	false	Scan hidden items in Exchange repositories, when set to true.
Discover.Exchange.UseSecureHttpConnections	true	Specifies whether connections to Exchange repositories and Active Directory are secure when using the Exchange Web Services crawler.
Discover.IgnorePstMessageClasses	IM.Appointment, IM.Contact, IM.Tack, MERRI. IM.Note.IR, REPORT. IPM.Note. IPNRN.	This setting specifies a comma-separated list of .pst message classes. All items in a .pst file that have a message class in the list will be ignored (no attempt will be made to extract the .pst item). This setting is case-sensitive.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Discover.IncludePstMessageClasses	IPM.Note	This setting specifies a comma-separated list of .pst message classes. All items in a .pst file that have a message class in the list will be included.  When both the include setting and the ignore setting are defined, Discover.IncludePstMessageClasses takes precedence.
Discover.PollInterval	10000	Specifies the time interval (in milliseconds) at which Enforce retrieves data from the Discover monitor while scanning.
Discover.Sharepoint.FetchACL	true	Turns off ACL fetching for integrated SharePoint scans. The default value is true (on).
Discover. Validate SSL Certificates	false	Set to true to enable validation of the SSL certificates for the HTTPS connections for SharePoint and Exchange targets. When validation is enabled, scanning SharePoint or Exchange servers using self-signed or untrusted certificates fails. If the SharePoint web application or Exchange server is signed by a certificate issued by a certificate authority (CA), then the server certificate or the server CA certificate must reside in the Java trusted keystore used by the Discover Server. If the certificate is not in the keystore, you must import it manually using the keytool utility.  See "Importing SSL certificates to Enforce or Discover servers" on page 197.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
EDM.MatchCountVariant	2	Specifies how matches are counted.  1 - Counts the total number of token sets matched.  2 - Counts the number of unique token sets matched (default).
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
EDM.MaximumNumberOfMatchesToReturn	100	Defines a top limit on the number of matches returned from each RAM index search.
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
EDM.RunProximityLogic	true	If true, runs the token proximity check.
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
EDM.SimpleTextProximityRadius	35	Number of tokens that are evaluated together when the proximity check is enabled.
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
EDM.TokenVerifierEnabled	false	Reserved for future use. Setting to true has no effect.
EndpointCommunications. AllConnInboundDataThrottleInKBPS	0	If enabled, limits the transfer rate of all inbound traffic in kilobits per second.
		Default is disabled.
		Changes to this setting apply to all new connections. Changes do not affect existing connections.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
EndpointCommunications. AllConnOutboundDataThrottleInKBPS	0	If enabled, limits the transfer rate of all inbound traffic in kilobits per second.
		Default is disabled.
		Changes to this setting apply to all new connections. Changes do not affect existing connections.
EndpointCommunications. ApplicationHandshakeTimeoutInSeconds	60	Maximum time for server to wait for each round trip during application handshake communications before closing the server-to-agent connection.
		Applies to the duration of time between when the agent accepts the TCP connection and when the agent receives the handshake message. This duration includes the SSL handshake and the agent receiving the HTTP headers. If the process exceeds the specified duration, the connection closes.  Changes to this setting apply to all new connections.
		new connections. Changes do not affect existing connections.
EndpointCommunications.MaxActiveAgentsPerServer	90000	Sets the maximum number of agents associated with a given server at any moment in time.
		This setting is implemented after the next Endpoint Server restart.
EndpointCommunications.  MaxActiveAgentsPerServerGroup	150000	Sets the maximum number of agents that will be associated with a given group of servers behind the same local load balancer at any moment in time. Used for maximum sizes of caches for internal endpoint features.  This setting is implemented after the next Endpoint Server restart.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
EndpointCommunications.MaxConcurrentConnections	90000	Sets the maximum number of simultaneous connections to allow.
		Changes to this setting apply to all new connections. Changes do not affect existing connections.
EndpointCommunications.  MaxConnectionLifetimeInSeconds	86400 (1 day)	Sets the maximum time to allow a connection to remain open. Do not set connections to remain open indefinitely. Connections that close ensure that SSL session keys are frequently updated to improve security. This timeout only applies during the normal operation phase of a connection, after the SSL handshake and application handshake phases of a connection.
		This setting is implemented immediately to all connections.
EndpointCommunications.ShutdownTimeoutInMillis	5000 (5 seconds)	Sets the maximum time to wait to gracefully close connections during shutdown before forcing connections to close.
		This setting is implemented immediately to all connections.
EndpointCommunications.SSLCipherSuites	TLS_RSA_WITH_ AES_128_CBC_SHA	Lists the allowed SSL cipher suites. Enter multiple entries, separated by commas.
		Changes to this setting apply to all new connections. Changes do not affect existing connections.
EndpointCommunications. SSLSessionCacheTimeoutInSeconds	86400	Sets the maximum SSL session entry lifetime in the SSL session cache.
		The default settings equals one day. This setting is implemented after the next Endpoint Server restart.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
EndpointMessageStatistics.MaxFileDetectionCount	100	The maximum number of times a valid file will be scanned. The file must not cause an incident. After exceeding this number, a system event is generated recommending that the file be filtered out.
EndpointMessageStatistics.MaxFolderDetectionCount	1800	The maximum number of times a valid folder will be scanned. The folder must not cause an incident. After exceeding this number, a system event is generated recommending that the file be filtered out.
EndpointMessageStatistics.MaxMessageCount	2000	The maximum number of times a valid message will be scanned. The message must not cause an incident. After exceeding this number, a system event is generated recommending that the file be filtered out.
EndpointMessageStatistics.MaxSetSize	3	The maximum list of hosts displayed from where valid files, folders, and messages come. When a system event for Endpoint/MessageStatists/MaxFetDetector/Count, Endpoint/MessageStatists/MaxFetder/Detector/Count or Endpoint/MessageStatists/MaxFetder/Detector/Count is generated, Symantec Data Loss Prevention lists the host machines where these system events were generated. This setting limits the number of hosts displayed in the list.
EndpointServer.Discover.ScanStatusBatchInterval	60000	The interval of time in milliseconds the Endpoint Server accumulates Endpoint Discover scan statuses before sending them to the Endpoint Server as a batch.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
		-
EndpointServer.Discover.ScanStatusBatchSize	1000	The number of scan statuses the Aggregator accumulates before sending them to the Enforce Server as a batch. The Endpoint Server forwards a batch of statuses to the Enforce Server when the status count reaches the configured value.
		The batch is forwarded to the Enforce Server when any of the thresholds for the following settings are met:
		EndpoinSeverDiscoverScanSatusBathInterval     EndpoinSeverDiscoverScanSatusBathSize
EndpointServer.EndpointSystemEventQueueSize	20000	The maximum number of system events that can be stored in the endpoint agent's queue to be sent to the Endpoint Server. If the database connection is lost or some other occurrence results in a massive number of system events, any additional system events that occur after this number is reached are discarded. This value can be adjusted according to memory requirements.
EndpointServer.MaxPercentage MemToStoreEndpointFiles	60	The maximum amount (in percentage) of memory to use to store shadow cache files.
EndpointServer.MaxTimeToKeepEndpointFilesOpen	20000	The time interval (in minutes) that the endpoint file is kept open or the file size can exceed the EndpointServer.MaxEndpointFileSize setting whichever occurs first.
EndpointServer.MaxTimeToWaitForWriter	1000	The maximum time (in milliseconds) that the agent will wait to connect to the server.
EndpointServer.NoOfRecievers	15	The number of endpoint shadow cache file receivers.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
EndpointServer.NoOfWriters	10	The number of endpoint shadow cache file writers.
FileReader.MaxFileSize	30M	The maximum size (in MB) of a message to be processed. Larger messages are truncated to this size.
FileReader.MaxFileSystemCrawlerMemory	30M	The maximum memory that is allocated for the File System Crawler. If this value is less than FileReader.MaxFileSize, then the greater of the two values is assigned.
FileReader.MaxReadGap	15	The time that a child process can have data but not have read anything before it stops sending heartbeats.
FileReader.ScheduledInterval	1000	The time interval (in milliseconds) between drop folder checks by the filereader. This affects Copy Rule, Packet Capture, and File System channels only.
FileReader.TempDirectory	Path to a secure directory as specified in the filereader.temp.io.dir attribute in the FileReader.properties configuration file.	A secure directory on the detection server in which to store temporary files for the File reader.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Icap.AllowHosts	any	The default value of "any" permits all systems to make a connection to the Network Prevent for Web Server on the ICAP service port. Replacing "any" with the IP address or Fully-Qualified Domain Name (FQDN) of one or more systems restricts ICAP connections to just those designated systems. To designate multiple systems, separate their IP addresses of FQDNs by commas.
Icap.AllowStreaming	false	If true, ICAP output is streamed to the proxy directly without buffering the ICAP request first.
Icap.BindAddress	0.0.0.0	IP address to which a Network Prevent for Web Server listener binds. When BindAddress is configured, the server will only answer a connection to that IP address. The default value of 0.0.0.0 is a wild card that permits listening to all available addresses including 127.0.0.1.
Icap.BufferSize	зк	The size (in kilobytes) of the memory buffer used for ICAP request streaming and chunking. The streaming can happen only if the request is larger than FileReader.MaxFileSize and the request has a Content-Length header.
Icap.DisableHealthCheck	false	If true, disables the ICAP periodic self-check. If false, enables the ICAP periodic self-check. This setting is useful for debugging to remove clutter produced by self-check requests from the logs.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Icap.EnableIncidentSuppression	true	If the parameter is set to true, Incident Suppression Cache for Gmail traffic on Mobile Prevent for Web is enabled. If the parameter is set to false, suppression is disabled.
Icap.EnableTrace	false	If set to true, protocol debug tracing is enabled once a folder is specified using the Icap.TraceFolder setting.
Icap.ExchangeActiveSyncCommandsToInspect	SendMail	A comma-separated, case-sensitive list of ActiveSync commands which need to be sent through Symantec Data Loss Prevention detection. If this parameter is left blank, ActiveSync support is disabled. If this parameter is set to "any", all ActiveSync commands are inspected.
Icap.LoadBalanceFactor	1	The number of web proxy servers that a Network Prevent for Webserver is able to communicate with. For example, if the server is configured to communicate with 3 proxies, set the Icap.LoadBalanceFactor value to 3.
Icap.IncidentSuppressionCacheCleanupInterval	120000	The time interval in milliseconds for running the Incident Suppression cache clean-up thread.
Icap.IncidentSuppressionCacheTimeout	120000	The time in miliseconds to invalidate the Incident Suppression cache entry.
Icap.SpoolFolder		This value is needed for ICAP Spools.
Icap.TraceFolder		The fully qualified name of the folder or directory where protocol debug trace data is stored when the lcap.EnableTrace setting is true. By default, the value for this setting is left blank.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
IncidentDetection.IncidentLimitResetTime	86400000	Specifies the time frame (in milliseconds) used by the IncidentDetection.MaxIncidentsPerPolicy setting. The default setting 86400000 equals one day.
IncidentDetection.MaxContentLength	2000000	Applies only to regular expression rules. On a per-component basis, only the first MaxContentLength number of characters are scanned for violations. The default (2,000,000) is equivalent to > 1000 pages of typical text. The limiter exists to prevent regular expression rules from taking too long.
IncidentDetection.MaxIncidentsPerPolicy	10000	Defines the maximum number of incidents detected by a specific policy on a particular monitor within the time-frame specified in the IncidentDetectionIncidentTimeLimitResetTime. The default is 10,000 incidents per policy per time limit.
IncidentDetection.MessageWaitSevere	240	The number of minutes to wait before sending a severe system event about message wait times.
IncidentDetection.MessageWaitWarning	60	The number of minutes to wait before sending a warning system event about message wait times.

Detection server advanced settings (continued) **Table 10-9** 

	server advanced setti	
Setting	Default	Description
IncidentDetection.MinNormalizedSize	30	This setting applies to IDM detection. It MUST be kept in sync with the corresponding setting in the Indexer.properties file on the Enforce Server (which applies to indexing). Derivative detections only apply to messages when their normalized content is greater than this setting. If the normalized content size is less than this setting, IDM detection does a straight binary match.
IncidentDetection.patternConditionMaxViolations	100	The maximum number of pattern violations highlighted by detection. The exact number of matches may still be 'correct' but only the first 'patternConditionMaxViolations' are marked up in reporting. Increasing this number increases the size of incidents and potentially slows down the incident snapshot report.
IncidentDetection.StopCachingWhenMemoryLowerThan	400M	Instructs Detection to stop caching tokenized and cryptographic content between rule executions if the available JVM memory drops below this value (in megabytes). Setting this attribute to 0 enables caching regardless of the available memory and is not recommended because OutOfMemoryErrors may occur.  Setting this attribute to a value close to, or larger than, the value of the -Xmx option in BoxMonitor.FileReaderMemory effectively disables the caching.  Note that setting this value too low can have severe performance consequences.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
ncidentDetection.TrialMode	false	Prevention trial mode setting to generate prevention incidents without having a prevention setup.
		If true, SMTP incidents coming from the Copy Rule and Packet Capture channels appear as if they were prevented and HTTP incidents coming from Packet Capture channel appear as if they were prevented.
IncidentWriter.BacklogInfo	1000	The number of incidents that collect in the log before an information level message about the number of messages is generated.
IncidentWriter.BacklogSevere	10000	The number of incidents that collect in the log before a severe level message about the number of messages is generated.
IncidentWriter.BacklogWarning	3000	The number of incidents that collect in the log before a warning level message about the number of messages is generated.
IncidentWriter.ResolveIncidentDNSNames	false	If true, only recipient host names are resolved from IP.
IncidentWriter.ShouldEncryptContent	true	If true, the monitor will encrypt the body of every message, message component and cracked component before writing to disk or sending to Enforce.
Keyword.TokenVerifierEnabled	false	Default is disabled ("false").
		If enabled ("true"), the server validates tokens for Asian language keywords (Chinese, Japanese, and Korean).
		See "Enabling and using CJK token verification for server keyword matching" on page 593.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
L7.cleanHttpBody	true	If true, the HTML entity references are replaced with spaces.
L7.DefaultBATV	Standard	This setting determines the tagging scheme that Network Prevent for Email uses to interpret Bounce Address Tag Validation (BATV) tags in the MAIL FROM header of a message. If this setting is "Standard" (the default), Network Prevent uses the tagging scheme described in the BATV specification (see http://todsietf.org/htm/ktaft-levine-mass-batv-02). Change this setting to "Ironport" to enable compatibility with the IronPort proxy's implementation of BATV tagging.
L7.DefaultUrlEncodedCharset	UTF-8	Defines the default character set to be used in decoding query parameters or URL-encoded body when the character set information is missing from the header.
L7.discardDuplicateMessages	true	If true, the Monitor ignores duplicate messages based on the messageID.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
L7.ExtractBATV	true	If true (the default), Network Prevent for Email interprets Bounce Address Tag Validation (BATV) tags that are present in the MAIL FROM header of a message. This allows Network Prevent to include a meaningful sender address in incidents that are generated from messages having BATV tags. If this setting is false, Network Prevent for Email does not interpret BATV tags, and a message that contains BATV tags may generate an incident that has an unreadable sender address.  See http://tooksietf.org/html/draft-levine-mass-batv-02 for more information about BATV.
L7.httpClientIdHeader		The sender identifier header name. The default setting is X-Forwarded-For.
L7.MAX_NUM_HTTP_HEADERS	30	If any HTTP message that contains more than the specified header lines, it is discarded.
L7.maxWordLength	30	The maximum word length (in characters) allowed in UTCP string extraction.
L7.messageIDCacheCleanupInterval	600000	The length of time that the messageID is cached. The system will not cache duplicate messages during this time period if the L7.discardDuplicateMessages setting is set to true.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
L7.minSizeOfGetUrl	100	The minimum size of the GET URL to process. HTTP GET actions are not inspected by Symantec Data Loss Prevention for policy violations if the number of bytes in the URL is less than the value of this setting. For example, with the default value of 100, no detection check is performed when a browser displays the Symantec web site at: http://www.symantec.com/index.jsp. The reason is that the URL contains only 33 characters, which is less than the 100 minimum.
		Note: Other request types such as POST or PUT are not affected by L7.minSizeofGetURL. In order for Symantec Data Loss Prevention to inspect any GET actions at all, the L7.processGets setting must be set to true.
L7.processGets	true	If true, the GET requests are processed. If false, the GET requests are not processed. Note that this setting interacts with the L7.minSizeofGetURL setting.
Lexer.IncludePunctuation InWords	true	If true, punctuation characters internal to a token are considered during detection.  See "Configuring Advanced Server Settings for EDM policies" on page 400.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Lexer.MaximumNumber OfTokens	12000	Maximum number of tokens extracted from each message component for detection. Applicable to all detection technologies where tokenization is required (EDM, profiled DGM, and the system patterns supported by those technologies). Increasing the default value may cause the detection server to run out of memory and restart.  See "Configuring Advanced Server Settings for EDM policies" on page 400.
Lexer.MaxTokensPerMultiToken	10	Maximum number of sub-tokens that a multi-token cell can contain.  See "Configuring Advanced Server Settings for EDM policies" on page 400.
Lexer.MultiToken	true	If true cells containing spaces are treated as multi-tokens.  See "Configuring Advanced Server Settings for EDM policies" on page 400.
Lexer.StopwordLanguages	en	Enables the elimination of stop words for the specified languages. The default is English.  See "Configuring Advanced Server Settings for EDM policies" on page 400.
Lexer.Validate	true	If true, performs system pattern-specific validation.  See "Configuring Advanced Server Settings for EDM policies" on page 400.
MessageChain.ArchiveTimedOutStreams	false	Specifies whether messages should be archived to the temp folder

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
MessageChain.CacheSize	8	Limits the number of messages that can be queued in the message chains.
MessageChain.ContentDumpEnabled	false	
MessageChain.MaximumComponentTime	60,000	The time interval (in milliseconds) allowed before any chain component is restarted.
MessageChain.MaximumFailureTime	360000	Number of milliseconds that must elapse before restarting the filereader. This is tracked after a message chain error is detected and that message chain has not been recovered.
MessageChain.MaximumMessageTime	Varies	This setting varies between is either 600,000 or 1,800,000 depending on detection server type.  The maximum time interval (in milliseconds) that a message can remain in a message chain.
MessageChain.MemoryThrottlerReservedBytes	200,000,000	Number of bytes required to be available before a message is sent through the message chain. This setting can avoid out of memory issues. The default value is 200 MB. The throttler can be disabled by setting this value to 0.
MessageChain.MinimumFailureTime	30000	Number of milliseconds that must elapse before failure of a message chain is tracked. Failure eventually leads to restarting the message chain or file reader.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
MessageChain.NumChains	Varies	This number varies depending on detection server type. It is either 4 or 8.
		The number of messages, in parallel, that the filereader will process. Setting this number higher than 8 (with the other default settings) is not recommended. A higher setting does not substantially increase performance and there is a much greater risk of running out of memory. Setting this to less than 8 (in some cases 1) helps when processing big files, but it may slow down the system considerably.
MessageChain.StopProcessing WhenMemoryLowerThan	200M	Instructs Detection to stop drilling down into and processing sub-files if JVM available memory drops below this value. Setting this attribute to 0 will force sub-file processing, regardless of how little memory is available. Setting this attribute to a value close to or larger than the value of the -Xmx option in BoxMonitor.FileReaderMemory will effectively disable sub-file processing.
PacketCapture.DISCARD_HTTP_GET	true	If true, discards HTTP GET streams.
PacketCapture.DOES_DISCARD_ TRIGGER_STREAM_DUMP	false	If true, a list of tcpstreams is dumped to an output file in the log directory the first time a discard message is received.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
PacketCapture.ENDACE_BIN_PATH		To enable packet-capture using an Endace card, enter the path to the Endace /bin directory. Note that environment variables (such as %ENDACE_HOME%) cannot be used in this setting. For example: /usr/local/bin
PacketCapture.ENDACE_LIB_PATH		To enable packet-capture using an Endace card, enter the path to the Endace /lib directory. Note that environment variables (such as %ENDACE_HOME%) cannot be used in this setting. For example: /usr/local/lib
PacketCapture.ENDACE_XILINX_PATH		To enable packet-capture using an Endace card, enter the path to the Endace /xilinx directory. Note that environment variables (such as %ENDACE_HOME%) cannot be used in this setting. For example: /usr/local/dag/xilinx
PacketCapture.Filter		The default setting is tcp    ip proto 47    (vlan && (tcp    ip proto 47)).  When set to the default value all non-TCP packets are filtered out and not sent to Network Monitor.  The default value can be overridden using the tcpdump filter format documented in the tcpdump program. This setting allows specialists to create more exact filters (source and destination IPs for given ports).
PacketCapture.INPUT_SOURCE_FILE	/dummy.dmp	The full path and name of the input file.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
PacketCapture.IS_ARCHIVING_PACKETS	false	DO NOT USE THIS FIELD. Diagnostic setting that creates dumps of packets captured in packetcapture for later reuse. This feature is unsupported and does not have normal error checking. May cause repeated restarts on pcap.
PacketCapture.IS_ENDACE_ENABLED	false	To enable packet-capture using an Endace card, set this value to true.
PacketCapture.IS_FTP_RETR_ENABLED	false	If true, FTP GETS and FTP PUTS are processed. If false, only process FTP PUTS are processed.
PacketCapture.IS_INPUT_SOURCE_FILE	false	If true, continually reads in packets from a tcpdump formatted file indicated in INPUT_SOURCE_FILE. Set to dag when an Endace card is installed.
PacketCapture.IS_NAPATECH_ENABLED	false	To enable packet-capture using a Napatech card, set this value to true. The default setting is false.
PacketCapture.KERNEL_BUFFER_SIZE_I686	64M	For 32-bit Linux platforms, this setting specifies the amount of memory allocated to buffer network packets. Specify K for kilobytes or M for megabytes. Do not specify a value larger than 128M.
PacketCapture.KERNEL_BUFFER_SIZE_Win32	16M	For 32-bit Windows platforms, this setting specifies the amount of memory allocated to buffer network packets. Specify K for kilobytes or M for megabytes.
PacketCapture.KERNEL_BUFFER_SIZE_X64	64M	For 64-bit Windows platforms, this setting specifies the amount of memory allocated to buffer network packets. Specify K for kilobytes or M for megabytes.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
PacketCapture.KERNEL_BUFFER_SIZE_X86_64	64M	For 64-bit Linux platforms, this setting specifies the amount of memory allocated to buffer network packets. Specify K for kilobytes or M for megabytes. Do not specify a value larger than 64M.
PacketCapture.MAX_FILES_PER_DIRECTORY	30000	After the specified number of file streams are processed a new directory is created.
PacketCapture.MBYTES_LEFT_ TO_DISABLE_CAPTURE	1000	If the amount of disk space (in MB) left on the drop_pcap drive falls below this specification, packet capture is suspended. For example, if this number is 100, pcap will stop writing out drop_pcap files when there is less than 100 MB on the installed drive
PacketCapture.MBYTES_REQUIRED _TO_RESTART_CAPTURE	1500	The amount of disk space (in MB) needed on the drop_pcap drive before packet capture resumes again after stopping due to lack of space. For example, if this value is 150 and packet capture is suspended, packet capture resumes when more than 150 MB is available on the drop_pcap drive.
PacketCapture.NAPATECH_TOOLS_PATH		This setting specifies the location of the Napatech Tools directory. This directory is not set by default. If packet-capture is enabled for Napatech, enter the fully qualified path to the Napatech Tools installation directory.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
PacketCapture.NO_TRAFFIC_ALERT_PERIOD	86,400	The refresh time (in seconds), between no traffic alert messages. No traffic system events are created for a given protocol based on this time period. For instance, if this is set to 24*60*60 seconds, a new message is sent every day that there is no new traffic for a given protocol. Do not confuse with the per protocol traffic timeout, that tells us how long we initially go without traffic before sending the first alert.
PacketCapture.NUMBER_BUFFER_POOL_PACKETS	600000	The number of standard-sized preallocated packet buffers used to buffer and sort incoming traffic.
PacketCapture.NUMBER_JUMBO_POOL_PACKETS	1	The number of large-sized preallocated packet buffers that are used to buffer and sort incoming traffic.
PacketCapture.NUMBER_SMALL_ POOL_PACKETS	200000	The number of small-sized preallocated packet buffers that are used to buffer and sort incoming traffic.
PacketCapture.RING_CAPTURE_LENGTH	1518	Controls the amount of packet data that is captured. The default value of 1518 is sufficient to capture typical Ethernet networks and Ethernet over 802.1Q tagged VLANs.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
PacketCapture.RING_DEVICE_MEM	67108864	This setting is deprecated. Instead, use the PacketCapture.KERNEL_BUFFER_SIZE_I686 setting (for 32-bit Linux platforms) or the PacketCapture.KERNEL_BUFFER_SIZE_X86_64 setting (for 64-bit Linux platforms).
		Specifies the amount of memory (in bytes) to be allocated to buffer packets per device. (The default of 67108864 is equivalent to 64MB.)
PacketCapture.SIZE_BUFFER_POOL_PACKETS	1540	The size of standard-sized buffer pool packets.
PacketCapture.SIZE_JUMBO_POOL_PACKETS	10000	The size of jumbo-sized buffer pool packets.
PacketCapture.SIZE_SMALL_POOL_PACKETS	150	The size of small-sized buffer pool packets.
PacketCapture.SPOOL_DIRECTORY		The directory in which to spool streams with large numbers of packets. This setting is user defined.
PacketCapture.STREAM_WRITE_TIMEOUT	5000	The time (in milliseconds) between each count (StreamManager's write timeout)
ProfileIndex.CheckAvailableRAM	true	Specifies whether or not the amount of available RAM should be compared with a profile size before loading an EDM or IDM profile.  See "Configuring Advanced Server Settings for EDM policies" on page 400.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
ProfileIndex.MaximumInProcessIndexSize	100M	Specifies an upper limit for the maximum In Process index size. Profiles that exceed this size are loaded out of process by RMI.
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
ProfileIndex.MinimumMemoryReserve	600M	Specifies the memory reserved for out-of-process EDM and/or IDM algorithm execution. It is used to calculate the JVM heap size as index_size + MinumumMemoryReserve.  See "Configuring Advanced Server Settings for EDM policies"
ProfileIndex.ProcessTimeout	60000	on page 400.  The time interval (in milliseconds) for launching out of process indexing. If the process is not created within this amount of time then index loading fails.  See "Configuring Advanced Server"
		Settings for EDM policies" on page 400.
RequestProcessor.AddDefaultHeader	true	If true, adds a default header to every email processed (when in Inline SMTP mode). The default header is RequestProcessor.DefaultHeader. This header is added to all messages that pass through the system, i.e., if it is redirected, if another header is added, if the message has no policy violations then the header is added.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
RequestProcessor.AllowExtensions		The default setting is: 8BITMIME VRFY DSN HELP PIPELINING SIZE ENHANCEDSTATUSCODES STARTTLS
		This setting lists the SMTP protocol extensions that Network Prevent for Email can use when it communicates with other MTAs.
RequestProcessor.AllowHosts	any	The default value of any permits all systems to make connections to the Network Prevent for Email Server on the SMTP service port. Replacing any with the IP address or Fully-Qualified Domain Name (FQDN) of one or more systems restricts SMTP connections to just those designated systems. To designate multiple systems, separate their addresses with commas. Use only a comma to separate addresses; do not include any spaces between the addresses.
RequestProcessor.AllowUnauthenticatedConnections	false	The default value ensures that MTAs must authenticate with Network Prevent for Email for TLS communication.
RequestProcessor.Backlog	12	The backlog that the request processor specifies for the server socket listener.
Requestprocessor.BindAddress	0.0.0.0	IP address to which a Network Prevent for Email Server listener binds. When BindAddress is configured, the server will only answer a connection to that IP address. The default value of 0.0.0.0 is a wild card that permits listening to all available addresses including 127.0.0.1.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
Requestprocessor.DefaultCommandTimeout	300	Specifies the number of seconds the Network Prevent for Email Server waits for a response to an SMTP command before closing connections to the upstream and downstream MTAs. The default is 300 seconds. This setting does not apply to the "." command (the end of a DATA command). Do not modify the default without first consulting Symantec support.
Requestprocessor.DefaultPassHeader	See description	The default setting is: X-CFilter-Loop: Reflected.
		This is the default header that will be added if RequestProcessor. AddDefaultPassHeader is set to true, when in Inline SMTP mode. Must be in a valid header format, recommended to be an X header.
Requestprocessor.DotCommandTimeout	600	Specifies the number of seconds the Network Prevent for Email Server waits for a response to the "." command (the end of a DATA command) before closing connections to the upstream and downstream MTAs. The default is 600 seconds. Do not modify the default without first consulting Symantec support.
RequestProcessor.ForwardConnectionTimeout	20000	The timeout value to use when forwarding to an MTA.
RequestProcessor.KeyManagementAlgorithm	SunX509	The key management algorithm used in TLS communication.
RequestProcessor.MaxLineSize	1048576	The maximum size (in bytes) of data lines expected from an external MTA. If the data lines are larger than they are broken down to this size.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
RequestProcessor.Mode	ESMTP	Specifies the protocol mode to use (SMTP or ESMTP).
RequestProcessor.MTAResubmitPort	10026	This is the port number used by the request processor on the MTA to resend the SMTP message.
RequestProcessor.NumberOfDNSAttempts	4	The maximum number of DNS queries that Network Prevent for Email performs when it attempts to obtain mail exchange (MX) records for a domain. Network Prevent for Email uses this setting only if you have enabled MX record lookups.
RequestProcessor.RPLTimeout	360000	The maximum time in milliseconds allowed for email message processing by a Prevent server. Any email messages not processed during this time interval are passed on by the server.
RequestProcessor.ServerSocketPort	10025	The port number to be used by the SMTP monitor to listen for incoming connections from MTA.
RequestProcessor.TagHighestSeverity	false	When set to true, an additional email header that reports the highest severity of all the violated policies is added to the message. For example, if the email violated a policy of severity HIGH and a policy of severity LOW, it shows: X-DLP-MAX-Severity:HIGH.
RequestProcessor.TagPolicyCount.	false	When set to true an additional email header reporting the total number of policies that the message violates is added to the message. For example, if the message violates 3 policies a header reading: X-DLP-Policy-Count: 3 is added.

Detection server advanced settings (continued) **Table 10-9** 

Setting	Default	Description
RequestProcessor.TagScore	false	When set to true an additional email header reporting the total cumulative score of all the policies that the message violates is added to the message. Scores are calculated using the formula: High=4, Medium=3, Low=2, and Info=1. For example, if a message violates three policies, one with a severity of medium and two with a severity of low a header reading: X-DLP-Score: 7 is added.
RequestProcessor.TrustManagementAlgorithm	PKIX	The trust management algorithm that Network Prevent for Email uses when it validates certificates for TLS communication. You can optionally specify a built-in Java trust manager algorithm (such as SunX509 or SunPKIX) or a custom algorithm that you have developed.
RequestProcessorListener.ServerSocketPort	12355	The local TCP port that FileReader will use to listen for connections from RequestProcessor on a Network Prevent server.
SocketCommunication.BufferSize	8K	The size of the buffer that Network Prevent for Web uses to process ICAP requests. Increase the default value only if you need to process ICAP requests that are greater than 8K. Certain features, such as Active Directory authentication, may require an increas in buffer size.
UnicodeNormalizer.AsianCharRanges	default	Can be used to override the default definition of characters that are considered Asian by the detection engine. Must be either default, or a comma-separated list of ranges, for example: 11A80-11F9,3200-321E

Setting	Default	Description
UnicodeNormalizer.Enabled	on	Can be used to disable Unicode normalization. Enter <b>off</b> to disable.
UnicodeNormalizer.NewlineEliminationEnabled	on	Can be used to disable newline elimination for Asian languages. Enter <b>off</b> to disable.

**Table 10-9** Detection server advanced settings (continued)

See "About Symantec Data Loss Prevention administration" on page 55.

See "Advanced agent settings" on page 1414.

See "About the System Overview screen" on page 198.

See "Server Detail screen" on page 201.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

### About using load balancers in an endpoint deployment

You can use a load balancer to manage multiple Endpoint Servers, or a server pool. Adding Endpoint Servers to a load-balanced server pool enables Symantec Data Loss Prevention to use less bandwidth while managing more agents. When setting up a server pool to manage Endpoint Servers and agents, default Symantec Data Loss Prevention settings allow for communication between servers and agents. However, there are a number of load balancer settings that may affect how Endpoint Servers and agents communicate. You may have to make changes to advanced agent and server settings if the load balancer you use does not use default settings.

In general, load balancers should have the following settings applied to work best with Symantec Data Loss Prevention:

- 1-Gbps throughput
- SSL session server affinity
- 24 hour SSL session timeout period

The Endpoint Servers communicate most efficiently with agents when the load balancer is set up to use SSL session ID stickiness. (This protocol name may differ across load balancer brands.) Using session stickiness in a Symantec Data Loss Prevention implementation uses less bandwidth during the SSL handshake between agents and Endpoint Servers.

You review agent connection settings if the load balancer idle connection settings is not set to default. The load balancer idle connection setting can also be called connection timeout interval, clean idle connection, and so-on depending on the load balancer brand.

You can assess your Symantec Data Loss Prevention and load balancer settings by considering the following two scenarios:

- Default DLP settings
- Non-default DLP settings

Note: Contact Symantec Support before changing default advanced agent and advanced server settings.

Table 10-10 Default Symantec Data Loss Prevention settings scenario

Description	Resolution
Starting with version 12.5, Symantec Data Loss Prevention uses non-persistent connections by default. Using non-persitent connections means that Endpoint Servers close connections to agents after agents are idle for 30 seconds.	Consider how the agent idle timeout coincides with the load balancer close idle connection setting. If the load balancer is configured to close idle connections after less than 30 seconds, agents are prematurely disconnected from Endpoint Servers.  To resolve the issue, complete one of the following:  Change the agent idle timeout setting (EndpointCommunications.  IDLE_TIMEOUT_IN_SECONDS.int) to less than the close idle connection setting on the load balancer.  Increase the agent heartbeat setting (EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int) to be less than the load balancer close idle connections setting. The user must also increase the no traffic timeout setting (CommLayer.NO_TRAFFIC_TIMEOUT_IN_SECONDS.int) to a value greater than the agent heartbeat setting.

Table 10-11	Non-default Symantec Data Loss	Prevention settings scenario
-------------	--------------------------------	------------------------------

Description	Resolution
Consider how changes to default Symantec Data Loss Prevention settings affect how the load balancer handles idle and persistent agent connections. For example, if you change the idle timeout setting to 0 to create a persistent connection and you leave the default agent heartbeat setting (270 seconds), you must consider the idle connection setting on the load balancer. If the idle connection setting on the load balancer is less than 270 seconds, then agents are prematurely disconnected from Endpoint Servers.	To resolve the issue, complete one of the following:  Change the agent heartbeat (EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int) and no traffic timeout settings (CommLayer.NO_TRAFFIC_TIMEOUT_IN_SECONDS.int) to less than the load balancer idle connection setting.  Verify that the no traffic timeout setting is greater than the heartbeat setting.

See "Advanced server settings" on page 203.

See "Advanced agent settings" on page 1414.

# Chapter

# Managing log files

This chapter includes the following topics:

- About log files
- Log collection and configuration screen
- Configuring server logging behavior
- Collecting server logs and configuration files
- About log event codes

## **About log files**

Symantec Data Loss Prevention provides a number of different log files that record information about the behavior of the software. Log files fall into these categories:

- Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.
  - For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network. See "Operational log files" on page 244.
- Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain an Symantec Data Loss Prevention installation. However, Symantec Support may ask you to

provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary. See "Debug log files" on page 247.

- Installation log files record information about the Symantec Data Loss Prevention installation tasks that are performed on a particular computer. You can use these log files to verify an installation or troubleshoot installation errors. Installation log files reside in the following locations:
  - installdir\SymantecDLP\.install4j\installation.log stores the installation log for Symantec Data Loss Prevention.
  - installdir\oracle home\admin\protect\ stores the installation log for

See the Symantec Data Loss Prevention Installation Guide for more information.

#### Operational log files

The Enforce Server and the detection servers store operational log files in the \SymantecDLP\Protect\logs\ directory on Windows installations and in the /var/log/SymantecDLP/ directory on Linux installations. A number at the end of the log file name indicates the count (shown as 0 in Table 11-1).

Table 11-1 lists and describes the Symantec Data Loss Prevention operational log files.

Table 11-1	Operational log files
------------	-----------------------

Log file name	Description	Server
agentmanagement_webservices_access_0.log	Logs successful and failed attempts to access the Agent Management API web service.	Enforce Server
agentmanagement_webservices_soap_0.log	Logs the entire SOAP request and response for most requests to the Agent Management API web Service.	Enforce Server

Operational log files (continued) **Table 11-1** 

Log file name	Description	Server
boxmonitor_operational_0.log	The BoxMonitor process oversees the detection server processes that pertain to that particular server type.	All detection servers
	For example, the processes that run on Network Monitor are file reader and packet capture.	
	The BoxMonitor log file is typically very small, and it shows how the application processes are running.	
Classification_Operational_0.log	Logs the state of the Classification Detection Server, the web container, and requests.	Classification Detection Server
<pre>detection_operational_0.log</pre>	The detection operation log file provides details about how the detection server configuration and whether it is operating correctly.	All detection servers
detection_operational_trace_0.log	The detection trace log file provides details about each message that the detection server processes. The log file includes information such as:	All detection servers
	<ul> <li>The policies that were applied to the message</li> <li>The policy rules that were matched in the message</li> <li>The number of incidents the message generated.</li> </ul>	
machinelearning_training_operational_0.log	This log records information about the tasks, logs, and configuration files called on startup of the VML training process.	Enforce Server
manager_operational_0.log.	Logs information about the Symantec Data Loss Prevention manager process, which implements the Enforce Server administration console user interface.	Enforce Server

Operational log files (continued) **Table 11-1** 

Log file name	Description	Server
monitorcontroller_operational_0.log	Records a detailed log of the connections between the Enforce Server and all detection servers. It provides details about the information that is exchanged between these servers including whether policies have been pushed to the detection servers or not.	Enforce Server
<pre>SmtpPrevent_operational0.log</pre>	This operational log file pertains to SMTP Prevent only. It is the primary log for tracking the health and activity of a Network Prevent for Email system. Examine this file for information about the communication between the MTAs and the detection server.	SMTP Prevent detection servers
WebPrevent_Access0.log	This access log file contains information about the requests that are processed by Network and Mobile Prevent for Web detection servers. It is similar to web access logs for a proxy server.	<ul> <li>Network Prevent for Web detection servers</li> <li>Mobile Prevent for Web detection servers</li> </ul>
WebPrevent_Operational0.log	This operational log file reports on the operating condition of Network and Mobile Prevent for Web, such as whether the system is up or down and connection management.	<ul> <li>Network Prevent for Web detection servers</li> <li>Mobile Prevent for Web detection servers</li> </ul>
webservices_access_0.log	This log file records successful and failed attempts to access the Incident Reporting and Update Web Service.	Enforce Server

Log file name Description Server Enforce Server webservices soap 0.log Contains the entire SOAP request and response for most requests to the Reporting API Web Service. This log records all requests and responses except responses to incident binary requests. This log file is not created by default. See the Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide for more information.

Operational log files (continued) **Table 11-1** 

See "Network and Mobile Prevent for Web operational log files and event codes" on page 262.

See "Network and Mobile Prevent for Web access log files and fields" on page 264.

See "Network Prevent for Email log levels" on page 267.

See "Network Prevent for Email operational log codes" on page 267.

See "Network Prevent for Email originated responses and codes" on page 271.

#### Debug log files

The Enforce Server and the detection servers store debug log files in the \SymantecDLP\Protect\logs\ directory on Windows installations and in the /var/log/SymantecDLP/ directory on Linux installations. A number at the end of the log file name indicates the count (shown as 0 in debug log files).

The following table lists and describes the Symantec Data Loss Prevention debug log files.

**Table 11-2** Debug log files

Log file name	Description	Server
Aggregator0.log	This file describes communications between the detection server and the agents.	Endpoint detection
	Look at this log to troubleshoot the following problems:	servers
	<ul> <li>Connection to the agents</li> <li>To find out why incidents do not appear when they should</li> <li>If unexpected agent events occur</li> </ul>	
BoxMonitor0.log	This file is typically very small, and it shows how the application processes are running. The BoxMonitor process oversees the detection server processes that pertain to that particular server type.	All detection servers
	For example, the processes that run on Network Monitor are file reader and packet capture.	
ContentExtractionAPI_FileReader.log	Logs the behavior of the Content Extraction API file reader that sends requests to the plug-in host. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_filereader.xml.	Detection Server
ContentExtractionAPI_Manager.log	Logs the behavior of the Content Extraction API manager that sends requests to the plug-in host. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_manager.xml.	Enforce Server
ContentExtractionHost_FileReader.log	Logs the behavior of the Content Extraction File Reader hosts and plug-ins. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_filereader.xml.	Detection Server
ContentExtractionHost_Manager.log	Logs the behavior of the Content Extraction Manager hosts and plug-ins. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_manager.xml.	Enforce Server
DiscoverNative.log.0	Contains the log statements that the Network Discover native code emits. Currently contains the information that is related to .pst scanning. This log file applies only to the Network Discover Servers that run on Windows platforms.	Discover detection servers

Debug log files (continued) **Table 11-2** 

Log file name	Description	Server
FileReader0.log	This log file pertains to the file reader process and contains application-specific logging, which may be helpful in resolving issues in detection and incident creation. One symptom that shows up is content extractor timeouts.	All detection servers
flash_client_0.log	Logs messages from the Adobe Flex client used for folder risk reports by Network Discover.	Enforce Server
flash_server_remoting_0.log	Contains log messages from BlazeDS, an open-source component that responds to remote procedure calls from an Adobe Flex client. This log indicates whether the Enforce Server has received messages from the Flash client. At permissive log levels (FINE, FINER, FINEST), the BlazeDS logs contain the content of the client requests to the server and the content of the server responses to the client	Enforce Server
IncidentPersister0.log	This log file pertains to the Incident Persister process. This process reads incidents from the incidents folder on the Enforce Server, and writes them to the database. Look at this log if the incident queue on the Enforce Server (manager) grows too large. This situation can be observed also by checking the incidents folder on the Enforce Server to see if incidents have backed up.	Enforce Server
Indexer0.log	This log file contains information when an EDM profile or IDM profile is indexed. It also includes the information that is collected when the external indexer is used. If indexing fails then this log should be consulted.	Enforce Server (or computer where the external indexer is running)
jdbc.log	This log file is a trace of JDBC calls to the database. By default, writing to this log is turned off.	Enforce Server

Debug log files (continued) **Table 11-2** 

Log file name	Description	Server
machinelearning_native_filereader.log	This log file records the runtime category classification (positive and negative) and associated confidence levels for each message detected by a VML profile. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_filereader.xml.	Detection Server
machinelearning_training_0_0.log	This log file records the design-time base accuracy percentages for the ${\tt k-fold}$ evaluations for all VML profiles.	Enforce Server
machinelearning_training_native_manager.log	This log file records the total number of features modeled at design-time for each VML profile training run. The default logging level is "info" which is configurable using \Protect\config\log4cxx_config_manager.xml.	Enforce Server
MonitorController0.log	This log file is a detailed log of the connections between the Enforce Server and the detection servers. It gives details around the information that is exchanged between these servers including whether policies have been pushed to the detection servers or not.	Enforce Server
PacketCapture.log	This log file pertains to the packet capture process that reassembles packets into messages and writes to the drop_pcap directory. Look at this log if there is a problem with dropped packets or traffic is lower than expected. PacketCapture is not a Java process, so it does not follow the same logging rules as the other Symantec Data Loss Prevention system processes.	Network Monitor
PacketCapture0.log	This log file describes issues with PacketCapture communications.	Network Monitor
RequestProcessor0.log	This log file pertains to SMTP Prevent only. The log file is primarily for use in cases where SmtpPrevent0.log is not sufficient.	SMTP Prevent detection servers

Debug log files (continued) **Table 11-2** 

Log file name	Description	Server
ScanDetail-target-0.log	Where <i>target</i> is the name of the scan target. All white spaces in the target's name are replaced with hyphens. This log file pertains to Discover server scanning. It is a file by file record of what happened in the scan. If the scan of the file is successful, it reads success, and then the path, size, time, owner, and ACL information of the file scanned. If it failed, a warning appears followed by the file name.	Discover detection servers
tomcat\localhost.date.log	These Tomcat log files contain information for any action that involves the user interface. The logs include the user interface errors from red error message box, password failures when logging on, and Oracle errors (ORA –#).	Enforce Server
VontuIncidentPersister.log	This log file contains minimal information: stdout and stderr only (fatal events).	Enforce Server
VontuManager.log	This log file contains minimal information: stdout and stderr only (fatal events).	Enforce Server
VontuMonitor.log	This log file contains minimal information: stdout and stderr only (fatal events).	All detection servers
VontuMonitorController.log	This log file contains minimal information: stdout and stderr only (fatal events).	Enforce Server
VontuNotifier.log	This log file pertains to the Notifier service and its communications with the Enforce Server and the MonitorController service. Look at this file to see if the MonitorController service registered a policy change.	Enforce Server
VontuUpdate.log	This log file is populated when you update Symantec Data Loss Prevention.	Enforce Server

See "Network and Mobile Prevent for Web protocol debug log files" on page 266. See "Network Prevent for Email log levels" on page 267.

#### Log collection and configuration screen

Use the Logs screen (System > Servers > Logs) to collect log files or to configure logging behavior for any Symantec Data Loss Prevention server. The Logs screen contains two tabs that provide the following features:

- Collection—Use this tab to collect log files and configuration files from one or more Symantec Data Loss Prevention servers. See "Collecting server logs and configuration files" on page 257.
- Configuration—Use this tab to configure basic logging behavior for a Symantec Data Loss Prevention server, or to apply a custom log configuration file to a

See "Configuring server logging behavior" on page 252.

See "About log files" on page 243.

## Configuring server logging behavior

Use the Configuration tab of the Logs screen (System > Servers > Logs) to change logging configuration parameters for any server in the Symantec Data Loss Prevention deployment. The Select a Diagnostic Log Setting menu provides preconfigured settings for Enforce Server and detection server logging parameters. You can select an available preconfigured setting to define common log levels or to enable logging for common server features. The Select a Diagnostic Log Setting menu also provides a default setting that returns logging configuration parameters to the default settings used at installation time.

Table 11-3 describes the preconfigured log settings available for the Enforce Server. Table 11-4 describes the preconfigured settings available for detection servers.

Optionally, you can upload a custom log configuration file that you have created or modified using a text editor. (Use the Collection tab to download a log configuration file that you want to customize.) You can upload only those configuration files that modify logging properties (file names that end with Logging.properties). When you upload a new log configuration file to a server, the server first backs up the existing configuration file of the same name. The new file is then copied into the configuration file directory and its properties are applied immediately.

You do not need to restart the server process for the changes to take effect, unless you are directed to do so. As of the current software release, only changes to the PacketCaptureNativeLogging.properties and

DiscoverNativeLogging.properties files require you to restart the server process.

See "Server controls" on page 178.

Make sure that the configuration file that you upload contains valid property definitions that are applicable to the type of server you want to configure. If you make a mistake when uploading a log configuration file, use the preconfigured **Restore Defaults** setting to revert the log configuration to its original installed state.

The Enforce Server administration console performs only minimal validation of the log configuration files that you upload. It ensures that:

- Configuration file names correspond to actual logging configuration file names.
- Root level logging is enabled in the configuration file. This configuration ensures that some basic logging functionality is always available for a server.
- Properties in the file that define logging levels contain only valid values (such as info, fine, or warning).

If the server detects a problem with any of these items, it displays an error message and cancels the file upload.

If the Enforce Server successfully uploads a log configuration file change to a detection server, the administration console reports that the configuration change was submitted. If the detection server then encounters any problems when tries to apply the configuration change, it logs a system event warning to indicate the problem.

**Table 11-3** Preconfigured log settings for the Enforce Server

Select a Diagnostic Log Setting value	Description
Restore Defaults	Restores log file parameters to their default values.
Reporting API SOAP Logging	Logs the entire SOAP request and response message for most requests to the Reporting API Web Service. The logged messages are stored in the webservices_soap.log file, which is not created by default with new installations.
	You can use the contents of webservices_soap.log to diagnose problems when developing Reporting API Web Service clients. See the <i>Symantec Data Loss Prevention Reporting API Developers Guide</i> for more information.

Preconfigured log settings for the Enforce Server (continued) **Table 11-3** 

Select a Diagnostic Log Setting value	Description
Custom Attribute Lookup Logging	Logs diagnostic information each time the Enforce Server uses a lookup plug-in to populate custom attributes for an incident. Lookup plug-ins populate custom attribute data using LDAP, CSV files, or other data repositories. The diagnostic information is recorded in the Tomcat log file (c:\SymantecDLP\logs\tomcat\localhost.date.log) and the IncidentPersister_0.log file.  See "About custom attributes" on page 1076.  See "About using custom attributes" on page 1078.

**Table 11-4** Preconfigured log settings for detection servers

Select a Diagnostic Log Setting value	Detection server uses	Description
Restore Defaults	All detection servers	Restores log file parameters to their default values.
Discover Trace Logging	Network Discover Servers	Enables informational logging for Network Discover scans. These log messages are stored in FileReader0.log.

Preconfigured log settings for detection servers (continued) **Table 11-4** 

Select a Diagnostic Log Setting value	Detection server uses	Description
Detection Trace Logging	All detection servers	Logs information about each message that the detection server processes. This includes information such as:
		<ul> <li>The policies that were applied to the message</li> <li>The policy rules that were matched in the message</li> <li>The number of incidents that the message generated.</li> </ul>
		When you enable <b>Detection Trace Logging</b> , the resulting messages are stored in the
		detection_operational_trace_0.log file.
		Note: Trace logging can produce a large amount of data, and the data is stored in clear text format. Use trace logging only when you need to debug a specific problem.
Packet Capture Debug Logging	Network Monitor Servers	Enables basic debug logging for packet capture with Network Monitor. This setting logs information in the PacketCapture.log file.
		While this type of logging can produce a large amount of data, the <b>Packet Capture Debug Logging</b> setting limits the log file size to 50 MB and the maximum number of log files to 10.
		If you apply this log configuration setting to a server, you must restart the server process to enable the change.

Preconfigured log settings for detection servers (continued) **Table 11-4** 

Select a Diagnostic Log Setting value	Detection server uses	Description
Email Prevent Logging	Network Prevent for Email servers	Enables full message logging for Network Prevent for Email servers. This setting logs the complete message content and includes execution and error tracing information. Logged information is stored in the SmtpPrevent0.log file.
		Note: Trace logging can produce a large amount of data, and the data is stored in clear text format. Use trace logging only when you need to debug a specific problem.
		See "Network Prevent for Email operational log codes" on page 267.
		See "Network Prevent for Email originated responses and codes" on page 271.
ICAP Prevent Message Processing Logging	Network Prevent for Web servers	Enables operational and access logging for Network Prevent for Web. This setting logs information in the FileReader0.log file.
		See "Network and Mobile Prevent for Web operational log files and event codes" on page 262.
		See "Network and Mobile Prevent for Web access log files and fields" on page 264.

Follow this procedure to change the log configuration for a Symantec Data Loss Prevention server.

#### To configure logging properties for a server

- Click the **Configuration** tab if it is not already selected. 1
- If you want to configure logging properties for a detection server, select the 2 server name from the Select a Detection Server menu.

- If you want to apply preconfigured log settings to a server, select the configuration name from the Select a Diagnostic Configuration menu next to the server you want to configure.
  - See Table 11-3 and Table 11-4 for a description of the diagnostic configurations.
- If you instead want to use a customized log configuration file, click **Browse...** next to the server you want to configure. Then select the logging configuration file to use from the File Upload dialog, and click Open. You upload only logging configuration files, and not configuration files that affect other server features.

Note: If the Browse button is unavailable because of a previous menu selection. click Clear Form.

- Click Configure Logs to apply the preconfigured setting or custom log configuration file to the selected server.
- Check for any system event warnings that indicate a problem in applying configuration changes on a server.

See "Log collection and configuration screen" on page 252.

Note: The following debug log files are configured manually outside of the logging framework available through the Enforce Server administration console:

ContentExtractionAPI FileReader.log, ContentExtractionAPI Manager.log, ContentExtractionHost FileReader.log, ContentExtractionHost Manager.log, machinelearning native filereader.log, and

machinelearning training native manager.log. Refer to the entry for each of these log files in debug log file list for configuration details. See "Debug log files" on page 247.

## Collecting server logs and configuration files

Use the Collection tab of the Logs screen (System > Servers > Logs) to collect log files and configuration files from one or more Symantec Data Loss Prevention servers. You can collect files from a single detection server or from all detection servers, as well as from the Enforce Server computer. You can limit the collected files to only those files that were last updated in a specified range of dates.

The Enforce Server administration console stores all log and configuration files that you collect in a single ZIP file on the Enforce Server computer. If you retrieve files from multiple Symantec Data Loss Prevention servers, each server's files are stored in a separate subdirectory of the ZIP file.

Checkboxes on the **Collection** tab enable you to collect different types of files from the selected servers. Table 11-5 describes each type of file.

**Table 11-5** File types for collection

File type	Description
Operational Logs	Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files to troubleshoot any problems in the way the software integrates with other components of your system.
	For example, you can use operational log files to verify that a Network Prevent for Email Server communicates with a specific MTA on your network.
Debug and Trace Logs	Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain an Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.

File types for collection (continued) Table 11-5

File type	Description
Configuration Files	Use the <b>Configuration Files</b> option to retrieve both logging configuration files and server feature configuration files.
	Logging configuration files define the overall level of logging detail that is recorded in server log files. Logging configuration files also determine whether specific features or subsystem events are recorded to log files.
	For example, by default the Enforce console does not log SOAP messages that are generated from Reporting API Web service clients. The ManagerLogging.properties file contains a property that enables logging for SOAP messages.
	You can modify many common logging configuration properties by using the presets that are available on the <b>Configuration</b> tab.
	If you want to update a logging configuration file by hand, use the <b>Configuration Files</b> checkbox to download the configuration files for a server. You can modify individual logging properties using a text editor and then use the <b>Configuration</b> tab to upload the modified file to the server.
	See "Configuring server logging behavior" on page 252.
	The <b>Configuration Files</b> option retrieves the active logging configuration files and also any backup log configuration files that were created when you used the <b>Configuration</b> tab. This option also retrieves server feature configuration files. Server feature configuration files affect many different aspects of server behavior, such as the location of a syslog server or the communication settings of the server. You can collect these configuration files to help diagnose problems or verify server settings. However, you cannot use the <b>Configuration</b> tab to change server feature configuration files. You can only use the tab to change logging configuration files.

**Table 11-5** File types for collection (continued)

File type	Description
Agent Logs	Use the <b>Agent Logs</b> option to collect DLP agent service and operational log files from an Endpoint Prevent detection server. This option is available only for Endpoint Prevent servers. To collect agent logs using this option, you must have already pulled the log files from individual agents to the Endpoint Prevent detection server using a <b>Pull Logs</b> action.
	Use the <b>Agent List</b> screen to select individual agents and pull selected log files to the Endpoint Prevent detection server. Then use the <b>Agent Logs</b> option on this page to collect the log files.
	When the logs are pulled from the endpoint, they are stored on the Endpoint Server in an unencrypted format. After you collect the logs from the Endpoint Server, the logs are deleted from the Endpoint Server and are stored only on the Enforce Server. You can only collect logs from one endpoint at a time.
	See "Using the Agent List screen" on page 1460.
	See "12.0.x and earlier agent actions" on page 1485.

Operational, debug, trace log files are stored in the server identifier/logs subdirectory of the zip file. server\_identifier identifies the server that generated the log files, and it corresponds to one of the following values:

- If you collect log files from the Enforce Server, Symantec Data Loss Prevention replaces server identifier with the string Enforce. Note that Symantec Data Loss Prevention does not use the localized name of the Enforce Server.
- If a detection server's name includes only ASCII characters, Symantec Data Loss Prevention uses the detection server name for the server\_identifier value.
- If a detection server's name contains non-ASCII characters, Symantec Data Loss Prevention uses the string DetectionServer-ID-id number for the server identifier value. id number is a unique identification number for the detection server.

If you collect agent service log files or operational log files from an Endpoint Prevent server, the files are placed in the server identifier/agentlogs subdirectory. Each agent log file uses the individual agent name as the log file prefix.

Follow this procedure to collect log files and log configuration files from Symantec Data Loss Prevention servers.

#### To collect log files from one or more servers

- 1 Click the **Collection** tab if it is not already selected.
- Use the Date Range menu to select a range of dates for the files you want to 2 collect. Note that the collection process does not truncate downloaded log files in any way. The date range limits collected files to those files that were last updated in the specified range.
- To collect log files from the Enforce Server, select one or more of the checkboxes next to the **Enforce Server** entry to indicate the type of files you want to collect.
- To collect log files from one or all detection servers, use the **Select a Detection** Server menu to select either the name of a detection server or the Collect Logs from All Detection Servers option. Then select one or more of the checkboxes next to the menu to indicate the type of files you want to collect.
- 5 Click **Collect Logs** to begin the log collection process.

The administration console adds a new entry for the log collection process in the **Previous Log Collections** list at the bottom of the screen. If you are retrieving many log files, you may need to refresh the screen periodically to determine when the log collection process has completed.

**Note:** You can run only one log collection process at a time.

- 6 To cancel an active log collection process, click Cancel next to the log collection entry. You may need to cancel log collection if one or more servers are offline and the collection process cannot complete. When you cancel the log collection, the ZIP file contains only those files that were successfully collected.
- To download collected logs to your local computer, click **Download** next to the log collection entry.
- To remove ZIP files stored on the Enforce Server, click **Delete** next to a log collection entry.

See "Log collection and configuration screen" on page 252.

See "About log files" on page 243.

## About log event codes

Operational log file messages are formatted to closely match industry standards for the various protocols involved. These log messages contain event codes that describe the specific task that the software was trying to perform when the message was recorded. Log messages are generally formatted as:

Timestamp [Log Level] (Event Code) Event description [event parameters]

- See "Network and Mobile Prevent for Web operational log files and event codes" on page 262.
- See "Network Prevent for Email operational log codes" on page 267.
- See "Network Prevent for Email originated responses and codes" on page 271.

### Network and Mobile Prevent for Web operational log files and event codes

Network and Mobile Prevent for Web log file names use the format of WebPrevent Operational X.log (where X is a number). The number of files that are stored and their sizes can be specified by changing the values in the FileReaderLogging.properties file. This file is in the SymantecDLP\Protect\config directory. By default, the values are:

- com.vontu.icap.log.lcapOperationalLogHandler.limit = 5000000
- com.vontu.icap.log.lcapOperationalLogHandler.count = 5

Table 11-6 lists the Network and Mobile Prevent for Web-defined operational logging codes by category. The italicized part of the text contains event parameters.

**Table 11-6** Status codes for Network and Mobile Prevent for Web operational logs

Code	Text and Description		
Operat	Operational Events		
1100	Starting Mobile Prevent for Web		
1101	Shutting down Mobile Prevent for Web		
Connectivity Events			

Status codes for Network and Mobile Prevent for Web operational **Table 11-6** logs (continued)

Code	Text and Description
1200	Listening for incoming connections at icap_bind_address:icap_bind_port
	Where:
	<ul> <li>icap_bind_address is the Network and Mobile Prevent for Web bind address to which the server listens. This address is specified with the Icap.BindAddress Advanced Setting.</li> <li>icap_bind_port is the port at which the server listens. This port is set in the Server &gt; Configure page.</li> </ul>
1201	Connection (id=conn_id) opened from host(icap_client_ip:icap_client_port)
	Where:
	<ul> <li>conn_id is the connection ID that is allocated to this connection. This ID can be helpful in doing correlations between multiple logs.</li> <li>icap_client_ip and icap_client_port are the proxy's IP address and port from</li> </ul>
	which the connect operation to Network and Mobile Prevent for Web was performed.
1202	Connection (id=conn_id) closed (close_reason)
	Where:
	<ul> <li>conn_id is the connection ID that is allocated to the connect operation.</li> <li>close_reason provides the reason for closing the connection.</li> </ul>
1203	Connection states: REQMOD=N, RESPMOD=N, OPTIONS=N, OTHERS=N
	Where <i>N</i> indicates the number of connections in each state, when the message was logged.
	This message provides the system state in terms of connection management. It is logged whenever a connection is opened or closed.

Status codes for Network and Mobile Prevent for Web operational Table 11-6 logs (continued)

Code	Text and Description
5200	Failed to create listener at <pre>icap_bind_address:icap_bind_port</pre>
	Where:
	<ul> <li>icap_bind_address is the Network and Mobile Prevent for Web bind address to which the server listens. This address can be specified with the Icap.BindAddress Advanced Setting.</li> <li>icap_bind_port is the port at which the server listens. This port is set on the Server &gt; Configure page.</li> </ul>
5201	Connection was rejected from unauthorized host (host_ip:port)
	Where <i>host_ip</i> and <i>port</i> are the proxy system IP and port address from which a connect attempt to Network and Mobile Prevent for Web was performed. If the host is not listed in the Icap.AllowHosts Advanced setting, it is unable to form a connection.

See "About log files" on page 243.

## Network and Mobile Prevent for Web access log files and fields

Network and Mobile Prevent for Web log file names use the format of WebPrevent AccessX.log (where X is a number). The number of files that are stored and their sizes can be specified by changing the values in the FileReaderLogging.properties file. By default, the values are:

- com.vontu.icap.log.lcapAccessLogHandler.limit = 5000000
- com.vontu.icap.log.lcapAccessLogHandler.count = 5

A Network and Mobile Prevent for Web access log is similar to a proxy server's web access log. The "start" log message format is:

```
# Web Prevent starting: start time
```

Where start time format is date:time, for example:

13/Aug/2008:03:11:22:015-0700.

#### The description message format is:

```
# host ip "auth user" time stamp "request line" icap status code
request size "referer" "user agent" processing time(ms) conn id client ip
client port action code icap method code traffic source code
```

Table 11-7 lists the fields. The values of fields that are enclosed in quotes in this example are quoted in an actual message. If field values cannot be determined, the message displays - or "" as a default value.

Table 11-7 Network and Mobile Prevent for Web access log fields

Fields	Explanation	
host_ip	IP address of the host that made the request.	
auth_user	Authorized user for this request.	
time_stamp	Time that Network and Mobile Prevent receives the request.	
request_line	Line that represents the request.	
icap_status_code	ICAP response code that Network and Mobile Prevent sends by for this request.	
request_size	Request size in bytes.	
referrer	Header value from the request that contains the URI from which this request came.	
user_agent	User agent that is associated with the request.	
processing_time (milliseconds)	Request processing time in milliseconds. This value is the total of the receiving, content inspection, and sending times.	
conn_id	Connection ID associated with the request.	
client_ip	IP of the ICAP client (proxy).	
client_port	Port of the ICAP client (proxy).	
action_code	An integer representing the action that Network and Mobile Prevent for Web takes. Where the action code is one of the following:	
	■ 0 = UNKNOWN	
	■ 1 = ALLOW	
	■ 2 = BLOCK	
	■ 3 = REDACT	
	■ 4 = ERROR	
	■ 5 = ALLOW_WITHOUT_INSPECTION	
	■ 6 = OPTIONS_RESPONSE	
	■ 7 = REDIRECT	

Fields	Explanation	
icap_method_code	An integer representing the ICAP method that is associated with this request. Where the ICAP method code is one of the following	
	■ -1 = ILLEGAL ■ 0 = OPTIONS ■ 1 = REQMOD ■ 2 = RESPMOD ■ 3 = LOG	
traffic_source_code	An integer that represents the source of the network traffic. Where the traffic source code is one of the following:  0 = MOBILE 1 = WEB 2 = UNKNOWN	

**Table 11-7** Network and Mobile Prevent for Web access log fields (continued)

See "About log files" on page 243.

## Network and Mobile Prevent for Web protocol debug log files

To enable ICAP trace logging, set the Icap. EnableTrace Advanced setting to true and use the Icap. TraceFolder Advanced setting to specify a directory to receive the traces. Symantec Data Loss Prevention service must be restarted for this change to take effect.

Trace files that are placed in the specified directory have file names in the format: timestamp-conn\_id. The first line of a trace file provides information about the connecting host IP and port along with a timestamp. File data that is read from the socket is displayed in the format <<timestamp number of bytes read. Data that is written to the socket is displayed in the format >>timestamp

number of bytes written. The last line should note that the connection has been closed.

Note: Trace logging produces a large amount of data and therefore requires a large amount of free disk storage space. Trace logging should be used only for debugging an issue because the data that is written in the file is in clear text.

See "About log files" on page 243.

## Network Prevent for Email log levels

Network Prevent for Email log file names use the format of EmailPrevent OperationalX.log (where X is a number). The number of files that are stored and their sizes can be specified by changing the values in the FileReaderLogging.properties file. By default, the values are:

- com.vontu.mta.log.SmtpOperationalLogHandler.limit = 5000000
- com.vontu.mta.log.SmtpOperationalLogHandler.count = 5

At various log levels, components in the com.vontu.mta.rp package output varying levels of detail. The com.vontu.mta.rp.level setting specifies log levels in the RequestProcessorLogging.properties file which is stored in the SymantecDLP\Protect\config directory. For example, com.vontu.mta.rp.level = FINE specifies the FINE level of detail.

Table 11-8 describes the Network Prevent for Email log levels.

**Table 11-8** Network Prevent for Email log levels

Level	Guidelines		
INFO	General events: connect and disconnect notices, information on the messages that are processed per connection.		
FINE	Some additional execution tracing information.		
FINER	Envelope command streams, message headers, detection results.		
FINEST	Complete message content, deepest execution tracing, and error tracing.		

See "About log files" on page 243.

## Network Prevent for Email operational log codes

Table 11-9 lists the defined Network Prevent for Email operational logging codes by category.

Table 11-9 Status codes for Network Prevent for Email operational log

Code	Description		
Core Events			
1100	Starting Network Prevent for Email		
1101	Shutting down Network Prevent for Email		

Status codes for Network Prevent for Email operational log **Table 11-9** (continued)

Code	Description		
1102	Reconnecting to FileReader (tid=id)		
	Where id is the thread identifier.		
	The RequestProcessor attempts to re-establish its connection with the FileReader for detection.		
1103	Reconnected to the FileReader successfully (tid=id)		
	The RequestProcessor was able to re-establish its connection to the FileReader.		
Core Er	rors		
5100	Could not connect to the FileReader (tid=id timeout=.3s)		
	An attempt to re-connect to the FileReader failed.		
5101	FileReader connection lost (tid=id)		
	The RequestProcessor connection to the FileReader was lost.		
Connec	tivity Events		
1200	Listening for incoming connections (local=hostname)		
	Hostnames is an IP address or fully-qualified domain name.		
1201	Connection accepted (tid=id cid=N		
	<pre>local=hostname:port remote=hostname:port)</pre>		
	Where <i>N</i> is the connection identifier.		
1202	Peer disconnected (tid=id cid=N		
	local=hostname:port		
	remote=hostname:port)		
1203	Forward connection established (tid=id cid=N		
	local=hostname:port		
	remote=hostname:port)		
1204	Forward connection closed (tid=id cid=N		
	local=hostname:port		
	remote=hostname:port)		

Status codes for Network Prevent for Email operational log *(continued)* **Table 11-9** 

Code	Description			
1205	Service connection closed (tid=id cid=N local=hostname:port remote=hostname:port messages=1 time=0.14s)			
Connec	tivity Errors			
5200	Connection is rejected from the unauthorized host (tid=id local=hostname:port remote=hostname:port)			
5201	Local connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)			
5202	Sender connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)			
5203	Forwarding connection error (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)			
5204	Peer disconnected unexpectedly (tid=id cid=N local=hostname:port remote=hostname:port reason=Explanation)			
5205	Could not create listener (address=local=hostname:port reason=Explanation)			
5206	Authorized MTAs contains invalid hosts: hostname, hostname,			
5207	MTA restrictions are active, but no MTAs are authorized to communicate with this host			
5208	TLS handshake failed (reason=Explanation tid=id cid=N local=hostname remote=hostname)			

**Table 11-9** Status codes for Network Prevent for Email operational log (continued)

Code	Description		
5209	TLS handshake completed (tid=id cid=N local=hostname remote=hostname)		
5210	All forward hosts unavailable (tid=id cid=N reason=Explanation)		
5211	DNS lookup failure (tid=id cid=N NextHop=hostname reason=Explanation)		
5303	Failed to encrypt incoming message (tid=id cid=N local=hostname remote=hostname)		
5304	Failed to decrypt outgoing message (tid=id cid=N local=hostname remote=hostname)		

#### Message Events

1300

Message complete (cid=N message id=3 dlp id=message identifier size=number sender=email address recipient count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N

#### Where:

- Recipient\_count is the total number of addressees in the To, CC, and BCC
- Response is the Network Prevent for Email response which can be one of: PASS, BLOCK, BLOCK AND REDIRECT, REDIRECT, MODIFY, or ERROR.
- Thee status is an Enhanced Status code.
  - See "Network Prevent for Email originated responses and codes" on page 271.
- The rtime is the time in seconds for Network Prevent for Emailto fully receive the message from the sending MTA.
- The dtime is the time in seconds for Network Prevent for Email to perform detection on the message.
- The mtime is the total time in seconds for Network Prevent for Email to process the message Message Errors.

#### Message Errors

**Table 11-9** Status codes for Network Prevent for Email operational log (continued)

Code	Description		
5300	Error while processing message (cid=N message_id=header_ID dlp_id=message_identifier size=0 sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N reason=Explanation  Where header_ID is an RFC 822 Message-Id header if one exists.		
5301	Sender rejected during re-submit		
5302	Recipient rejected during re-submit		

See "About log files" on page 243.

## Network Prevent for Email originated responses and codes

Network Prevent for Email originates the following responses. Other protocol responses are expected as Network Prevent for Email relays command stream responses from the forwarding MTA to the sending MTA. Table 11-10 shows the responses that occur in situations where Network Prevent must override the receiving MTA. It also shows the situations where Network Preventgenerates a specific response to an event that is not relayed from downstream.

"Enhanced Status" is the RFC1893 Enhanced Status Code associated with the response.

Network Prevent for Email originated responses Table 11-10

Code	Enhanced Status	Text	Description
250	2.0.0	Ok: Carry on.	Success code that Network Prevent for Email uses.
221	2.0.0	Service closing.	The normal connection termination code that Network Prevent for Email generates if a QUIT request is received when no forward MTA connection is active.

 Table 11-10
 Network Prevent for Email originated responses (continued)

Code	Enhanced Status	Text	Description
451	4.3.0	Error: Processing error.	This "general, transient" error response is issued when a (potentially) recoverable error condition arises. This error response is issued when a more specific error response is not available. Forward connections are sometimes closed, and their unexpected termination is occasionally a cause of a code 451, status 4.3.0. However sending connections should remain open when such a condition arises unless the sending MTA chooses to terminate.
421	4.3.0	Fatal: Processing error. Closing connection.	This "general, terminal" error response is issued when a fatal, unrecoverable error condition arises. This error results in the immediate termination of any sender or receiver connections.
421	4.4.1	Fatal: Forwarding agent unavailable.	That an attempt to connect the forward MTA was refused or otherwise failed to establish properly.
421	4.4.2	Fatal: Connection lost to forwarding agent.	Closing connection. The forwarded MTA connection is lost in a state where further conversation with the sending MTA is not possible. The loss usually occurs in the middle of message header or body buffering. The connection is terminated immediately.
451	4.4.2	Error: Connection lost to forwarding agent.	The forward MTA connection was lost in a state that may be recoverable if the connection can be re-established. The sending MTA connection is maintained unless it chooses to terminate.
421	4.4.7	Error: Request timeout exceeded.	The last command issued did not receive a response within the time window that is defined in the RequestProcessor.DefaultCommandTimeout. (The time window may be from RequestProcessor.DotCommandTimeout if the command issued was the "."). The connection is closed immediately.

Table 11-10 Network Prevent for Email originated responses (continued)

Code	Enhanced Status	Text	Description
421	4.4.7	Error: Connection timeout exceeded.	The connection was idle (no commands actively awaiting response) in excess of the time window that is defined in RequestProcessor.DefaultCommandTimeout.
501	5.5.2	Fatal: Invalid transmission request.	A fatal violation of the SMTP protocol (or the constraints that are placed on it) occurred. The violation is not expected to change on a resubmitted message attempt. This message is only issued in response to a single command or data line that exceeds the boundaries that are defined in RequestProcessor.MaxLineLength.
502	5.5.1	Error: Unrecognized command.	Defined but not currently used.
550	5.7.1	User Supplied.	This combination of code and status indicates that a Blocking response rule has been engaged. The text that is returned is supplied as part of the response rule definition.

Note that a 4xx code and a 4.x.x enhanced status indicate a temporary error. In such cases the MTA can resubmit the message to the Network Prevent for Email Server. A 5xx code and a 5.x.x enhanced status indicate a permanent error. In such cases the MTA should treat the message as undeliverable.

See "About log files" on page 243.

# Using Symantec Data Loss Prevention utilities

This chapter includes the following topics:

- About the Symantec Data Loss Prevention utilities
- About Endpoint utilities
- About the Environment Check Utility
- About DBPasswordChanger

## **About the Symantec Data Loss Prevention utilities**

Symantec provides a suite of utilities to help users accomplish those tasks that need to be done on an infrequent basis. The utilities are typically used to perform troubleshooting and maintenance tasks. They are also used to prepare data and files for use with the Symantec Data Loss Prevention software.

The Symantec Data Loss Prevention utilities are provided for both Windows and Linux operating systems. You use the command line to run the utilities on both operating systems. The utilities operate in a similar manner regardless of operating system.

Table 12-1 describes how and when to use each utility.

**Table 12-1** Symantec Data Loss Prevention utilities

Name	Description
Environment Check Utility	Audits the environment of a Symantec Data Loss Prevention server system and gathers information into a ZIP file. Symantec Support can use the ZIP file to troubleshoot problems.  See "About the Environment Check Utility" on page 276.
DBPasswordChanger	Changes the encrypted password that the Enforce Server uses to connect to the Oracle database.  See "About DBPasswordChanger" on page 279.
sslkeytool	Generates custom authentication keys to improve the security of the data that is transmitted between the Enforce Server and detection servers. The custom authentication keys must be copied to each Symantec Data Loss Prevention server.
	See the topic "About the sslkeytool utility and server certificates" in the <i>Symantec Data Loss Prevention Installation Guide</i> .
SQL Preindexer	Indexes an SQL database or runs an SQL query on specific data tables within the database. This utility is designed to pipe its output directly to the Remote EDM Indexer utility.
	See "About the SQL Preindexer" on page 433.
Remote EDM Indexer	Converts a comma-separated or tab-delimited data file into an exact data matching index. The utility can be run on a remote machine to provide the same indexing functionality that is available locally on the Enforce Server.
	This utility is often used with the SQL Preindexer. The SQL Preindexer can run an SQL query and pass the resulting data directly to the Remote EDM Indexer to create an EDM index.
	See "About the Remote EDM Indexer" on page 433.

## **About Endpoint utilities**

Table 12-2 describes those utilities that apply to the Endpoint products.

See "About Endpoint tools" on page 1523.

**Table 12-2 Endpoint utilities** 

Name	Description
Service_Shutdown.exe	This utility enables an administrator to turn off both the agent and the watchdog services on an endpoint. (As a tamper-proofing measure, it is not possible for a user to stop either the agent or the watchdog service.)  See "Shutting down the agent and the watchdog services" on page 1525.
Vontu_sqlite3.exe	This utility provides an SQL interface that enables you to view or modify the encrypted database files that the Symantec DLP Agent uses. Use this tool when you want to investigate or make changes to the Symantec Data Loss Prevention files.  See "Inspecting the database files accessed by the agent" on page 1526.
Logdump.exe	This tool lets you view the Symantec DLP Agent extended log files, which are hidden for security reasons.  See "Viewing extended log files" on page 1527.
Start_agent	This utility enables an administrator to start agents running on Mac endpoints that have been shut down using the shutdown task.  See "Starting DLP Agents that run on Mac endpoints" on page 1531.

## **About the Environment Check Utility**

The Environment Check Utility (ECU) validates the environment in which Symantec Data Loss Prevention servers operate. The ECU is a troubleshooting tool that is installed with the Enforce Server and detection servers. In most cases information is collected from both the Enforce Server and its detection servers. Certain checks are performed only when you run the utility on the Enforce Server.

See Table 12-3 for a description of which tasks are performed on Enforce Servers and detection servers.

Table 12-3	Environment Check Utility tasks
------------	---------------------------------

Task	Server Type
<ul> <li>Checks and displays the Windows or Linux operating system version.</li> <li>Verifies that required Symantec Data Loss Prevention services are running.</li> <li>Displays the full Symantec Data Loss Prevention version number.</li> <li>Checks the host configuration file and writes the configuration to a log file.</li> </ul>	Enforce Server or detection server
<ul> <li>Checks for the existence of the System Account user that was created during the Enforce Server installation.</li> <li>Checks the stored settings for each registered detection server and writes the information to the /SymantecDLP/Protect/ECU/eculogs/monitorSettings directory.</li> <li>Checks the Oracle database by exercising the Symantec Data Loss Prevention Notification and Lock Manager services.</li> <li>Checks the network connection from the Enforce Server to each registered detection server.</li> </ul>	Enforce Server

If you experience problems with your installation, Symantec Support may ask you to run this utility to collect information about the system environment.

## Running the Environment Check Utility on Windows

If the default installation directory was used, the Environment Check Utility is located in the c:\SymantecDLP\Protect\ECU directory.

#### To run the ECU on Windows

- From the Windows Start menu, select Run and type cmd in the resulting Run dialog box to open a command prompt window.
- 2 Go to the ECU folder (c:\SymantecDLP\Protect\ECU if you installed in the default location).
- 3 Execute the utility:

EnvironmentCheckUtility.exe

See "About Environment Check Utility output" on page 278.

## Running the Environment Check Utility on Linux

If the default installation directory was used, the Environment Check Utility is located in the /opt/SymantecDLP/Protect/ECU directory.

#### To run the ECU on Linux

Log on as the protect user by typing:

su protect

2 Go to the ECU directory. If you used the defaults during installation, type:

cd /opt/SymantecDLP/Protect/ECU

3 Execute the utility:

./EnvironmentCheckUtility

See "About Environment Check Utility output" on page 278.

### About Environment Check Utility output

When you run the Environment Check Utility, it generates an eculogs.zip file in the ECU subdirectory. This ZIP file contains several files with system information. If the utility runs on the Enforce Server computer, it also generates a subdirectory named eculogs\monitorSettings that contains information about each registered detection server.

The output files stored in <code>eculogs.zip</code> are as follows:

- ECUoutput.txt contains the test results (pass or fail) and possible reasons for the test failures.
- ecu error log.txt records any errors that occurred during the tests that the utility ran.
- ecu HostFileLog.txt contains a dump of the contents of the host file.
- server nameSettings.txt files record the settings of registered detection servers. These files, and eculogs/monitorSettings directory are generated only on the Enforce Server computer.

After the eculogs.zip file is created, send it to Symantec Support for further analysis.

See "About log files" on page 243.

## About DBPasswordChanger

Symantec Data Loss Prevention stores encrypted passwords to the Oracle database in a file that is called DatabasePassword.properties, located in

c:\SymantecDLP\Protect\config (Windows)

or/opt/SymantecDLP/Protect/config (Linux). Because the contents of the file are encrypted, you cannot directly modify the file. The DBPasswordChanger utility changes the stored Oracle database passwords that the Enforce Server uses.

Before you can use DBPasswordChanger to change the password to the Oracle database you must:

- Shut down the Enforce Server.
- Change the Oracle database password using Oracle utilities.

See "Example of using DBPasswordChanger" on page 279.

### DBPasswordChanger syntax

The DBPasswordChanger utility uses the following syntax:

DBPasswordChanger password file new oracle password

All command-line parameters are required. The following table describes each command-line parameter.

See "Example of using DBPasswordChanger" on page 279.

**Table 12-4** DBPasswordChanger command-line parameters

Parameter	Description
password_file	Specifies the file that contains the encrypted password. By default, this file is named ProtectPassword.properties and is stored in \SymantecDLP\Protect\config (Windows) or /opt/SymantecDLP/Protect/config (Linux).
new_oracle_password	Specifies the new Oracle password to encrypt and store.

## Example of using DBPasswordChanger

If Symantec Data Loss Prevention was installed in the default location, then the DBPasswordChanger utility is located at c:\Vontu\Protect\bin (Windows) or /opt/Vontu/Protect/bin (Linux). You must be an Administrator (or root) to run DBPasswordChanger.

For example, type:

DBPasswordChanger \Vontu\Protect\bin\DatabasePassword.properties protect oracle

See "DBPasswordChanger syntax" on page 279.

on

## Section

## Authoring policies

- Chapter 13. Introduction to policies
- Chapter 14. Overview of policy detection
- Chapter 15. Creating policies from templates
- Chapter 16. Configuring policies
- Chapter 17. Administering policies
- Chapter 18. Best practices for authoring policies
- Chapter 19. Detecting content using Exact Data Matching (EDM)
- Chapter 20. Detecting content using Indexed Document Matching (IDM)
- Chapter 21. Detecting content using Vector Machine Learning (VML)
- Chapter 22. Detecting content using data identifiers
- Chapter 23. Detecting content using keyword matching
- Chapter 24. Detecting content using regular expressions
- Chapter 25. Detecting international language content
- Chapter 26. Detecting file properties
- Chapter 27. Detecting email for data classification services

- Chapter 28. Detecting network and mobile incidents
- Chapter 29. Detecting endpoint events
- Chapter 30. Detecting described identities
- Chapter 31. Detecting synchronized identities
- Chapter 32. Detecting profiled identities
- Chapter 33. Supported file formats for detection
- Chapter 34. Library of system data identifiers
- Chapter 35. Library of policy templates

## Chapter

## Introduction to policies

This chapter includes the following topics:

- About Data Loss Prevention policies
- Policy components
- Policy templates
- Solution packs
- Policy groups
- Policy deployment
- Policy severity
- Policy authoring privileges
- Data Profiles
- User Groups
- Policy import and export
- Workflow for implementing policies
- Viewing, printing, and downloading policy details

## **About Data Loss Prevention policies**

You implement policies to detect and prevent data loss. A Symantec Data Loss Prevention policy combines detection rules and response actions. If a policy rule is violated, the system generates an incident that you can report and act on. The policy rules you implement are based on your information security objectives. The actions you take in response to policy violations are based on your compliance

requirements. The Enforce Server administration console provides an intuitive, centralized, Web-based interface for authoring policies.

See "Workflow for implementing policies" on page 293.

Table 13-1 describes the policy authoring features provided by Symantec Data Loss Prevention.

**Table 13-1** Policy authoring features

Feature	Description
Intuitive policy	The policy builder interface supports Boolean logic for detection configuration.
building	You can combine different detection methods and technologies in a single policy.
	See "Detecting data loss" on page 296.
	See "Best practices for authoring policies" on page 357.
Decoupled	The system stores response rules and policies as separate entities.
response rules	You can manage and update response rules without having to change policies; you can reuse response rules across policies.
	See "About response rules" on page 875.
Fine-grained policy	The system provides severity levels for policy violations.
reporting	You can report the overall severity of a policy violation by the highest severity.
	See "Policy severity" on page 289.
Centralized data	The system stores data and group profiles separate from policies.
and group profiling	This separation enables you to manage and update profiles without changing policies.
	See "Data Profiles" on page 291.
	See "User Groups" on page 292.
Template-based	The system provides 65 pre-built policy templates.
policy detection	You can use these templates to quickly configure and deploy policies.
	See "Policy templates" on page 286.
Policy sharing	The system supports policy template import and export.
	You can share policy templates across environments and systems.
	See "Policy import and export" on page 292.
Role-based access	The system provides role-based access control for various user and administrative functions.
control	You can create roles for policy authoring, policy administration, and response rule authoring.
	See "Policy authoring privileges" on page 290.

## **Policy components**

A valid policy has at least one detection or group rule with at least one match condition. Response rules are optional policy components.

Policy components describes Data Loss Prevention policy components.

Policy components **Table 13-2** 

Component	Use	Description
Policy group	Required	A policy must be assigned to a single Policy Group.
		See "Policy groups" on page 287.
Policy name	Required	The policy name must be unique within the Policy Group
		See "Manage and add policies" on page 345.
Policy rule	Required	A valid policy must contain at least one rule that declares at least one match condition.
		See "Policy matching conditions" on page 300.
Data Profile	May be required	A policy requires a Data Profile if a detection method in the policy requires it.
		Exact Data Matching (EDM), Indexed Document Matching (IDM), and Vector Machine Learning (VML) rules require a Data Profile.
		See "Data Profiles" on page 291.
User group	May be required	A policy requires a User Group only if a group method in the policy requires it.
		Synchronized DGM rules and exceptions require a User Group.
		See "User Groups" on page 292.
Policy description	Optional	A policy description helps users identify the purpose of the policy.
		See "Configuring policies" on page 326.
Policy label	Optional	A policy label helps Symantec Data Insight business users identify the purpose of the policy when using the Self-Service Portal.
		See "Configuring policies" on page 326.
Response Rule	Optional	A policy can implement one or more response rules to report and remediate incidents.
		See "About response rules" on page 875.

Component	Use	Description
Policy exception	Optional	A policy can contain one or more exceptions to exclude data from matching.  See "Exception conditions" on page 307.
Compound match conditions	Optional	A policy rule or exception can implement multiple match conditions.  See "Compound conditions" on page 308.

**Table 13-2** Policy components (continued)

## Policy templates

Symantec Data Loss Prevention provides policy templates to help you guickly deploy detection policies in your enterprise. You can share policies across systems and environments by importing and exporting policy rules and exceptions as templates.

Using policy templates saves you time and helps you avoid errors and information gaps in your policies because the detection methods are predefined. You can edit a template to create a policy that precisely suits your needs. You can also export and import your own policy templates.

Some policy templates are based on well-known sets of regulations, such as the Payment Card Industry Security Standard, Gramm-Leach-Bliley, California SB1386, and HIPAA. Other policy templates are more generic, such as Customer Data Protection, Employee Data Protection, and Encrypted Data. Although the regulation-based templates can help address the requirements of the relevant regulations, consult with your legal counsel to verify compliance.

See "Creating a policy from a template" on page 312.

Table 13-3 describes the system-defined policy templates provided by Symantec Data Loss Prevention.

**Table 13-3** System-defined policy templates

Policy template type	Description
US Regulatory Enforcement	See "US Regulatory Enforcement policy templates" on page 315.
UK and International Regulatory Enforcement	See "UK and International Regulatory Enforcement policy templates" on page 317.
Customer and Employee Data Protection	See "Customer and Employee Data Protection policy templates" on page 317.

Policy template type	Description
Confidential or Classified Data Protection	See "Confidential or Classified Data Protection policy templates" on page 319.
Network Security Enforcement	See "Network Security Enforcement policy templates" on page 320.
Acceptable Use Enforcement	See "Acceptable Use Enforcement policy templates" on page 320.
Imported Templates	See "Policy import and export" on page 292.
Classification for Enterprise Vault	See the Enterprise Vault Data Classification Services Implementation Guide.

**Table 13-3** System-defined policy templates (continued)

## Solution packs

Symantec Data Loss Prevention provides solution packs for several industry verticals. A solution pack contains configured policies, response rules, user roles, reports, protocols, and the incident statuses that support a particular industry or organization. For a list of available solution packs and instructions, refer to chapter 4, "Importing a solution pack" in the Symantec Data Loss Prevention Installation Guide. You can import one solution pack to the Enforce Server.

Once you have imported the solution pack, start by reviewing its policies. By default the solution pack activates the policies it provides.

See "Manage and add policies" on page 345.

## Policy groups

You deploy policies to detection servers using policy groups. Policy groups limit the policies, incidents, and detection mechanisms that are accessible to specific users.

Each policy belongs to one policy group. When you configure a policy, you assign it to a policy group. You can change the policy group assignment, but you cannot assign a policy to more than one policy group. You deploy policy groups to one or more detection servers.

The Enforce Server is configured with a single policy group called the **Default Policy Group.** The system deploys the default policy group to all detection servers. If you define a new policy, the system assigns the policy to the default policy group, unless you create and specify a different policy group. You can change the name

of the default policy group. A solution pack creates several policy groups and assigns policies to them.

After you create a policy group, you can link policies, Discover targets, and roles to the policy group. When you create a Discover target, you must associate it with a single policy group. When you associate a role with particular policy groups, you can restrict users in that role. Policies in that policy group detect incidents and report them to users in the role that is assigned to that policy group.

The relationship between policy groups and detection servers depends on the server type. You can deploy a policy group to one or more Network Monitor, Mobile Email Monitor, Network Prevent, Mobile Prevent, or Endpoint Servers. Policy groups that you deploy to an Endpoint Server apply to any DLP Agent that is registered with that server. The Enforce Server automatically associates all policy groups with all Network Discover Servers.

For Network Monitor and Network Prevent, each policy group is assigned to one or more Network Monitor Servers, Email Prevent Servers, or Web Prevent Servers. For Mobile Prevent, each policy group is assigned to one or more Mobile Prevent for Web Servers. For Network Discover, policy groups are assigned to individual Discover targets. A single detection server may handle as many policy groups as necessary to scan its targets. For Endpoint Monitor, policy groups are assigned to the Endpoint Server and apply to all registered DLP Agents.

See "Manage and add policy groups" on page 347.

See "Creating and modifying policy groups" on page 348.

## Policy deployment

You can use policy groups to organize and deploy your policies in different ways. For example, consider a situation in which your detection servers are set up across a system that spans several countries. You can use policy groups to ensure that a detection server runs only the policies that are valid for a specific location.

You can dedicate some of your detection servers to monitor internal network traffic and dedicate others to monitor network exit points. You can use policy groups to deploy less restrictive policies to servers that monitor internal traffic. At the same time, you can deploy stricter policies to servers that monitor traffic leaving your network.

You can use policy groups to organize policies and incidents by business units, departments, geographic regions, or any other organizational unit. For example, policy groups for specific departments may be appropriate where security responsibilities are distributed among various groups. In such cases, policy groups provide for role-based access control over the viewing and editing of incidents. You deploy policy groups according to the required division of access rights within your organization (for example, by business unit).

You can use policy groups for detection-server allocation, which may be more common where security departments are centralized. In these cases, you would carefully choose the detection server allocation for each role and reflect the server name in the policy group name. For example, you might name the groups Inbound and Outbound, United States and International, or Testing and Production.

In more complex environments, you might consider some combination of the following policy groups for deploying policies:

- Sales and Marketing US
- Sales and Marketing Europe
- Sales and Marketing Asia
- Sales and Marketing Australia, New Zealand
- Human Resources US
- Human Resources International
- Research and Development
- Customer service

Lastly, you can use policy groups to test policies before deploying them in production, to manage legacy policies, and to import and export policy templates.

See "Policy groups" on page 287.

See "About role-based access control" on page 84.

## Policy severity

When you configure a detection rule, you can select a policy severity level. You can then use response rules to take action based on a severity level. For example, you can configure a response rule to take action after a specified number of "High" severity violations.

See "About response rule conditions" on page 882.

The default severity level is set to "High," unless you change it. The default severity level applies to any condition that the detection rule matches. For example, if the default severity level is set to "High," every detection rule violation is labeled with this severity level. If you do not want to tag every violation with a specific severity, you can define the criteria by which a severity level is established. In this case the default behavior is overridden. For example, you can define the "High" severity level to be applied only after a specified number of condition matches have occurred.

See "Defining rule severity" on page 333.

In addition, you can define multiple severity levels to layer severity reporting. For example, you can set the "High" severity level after 100 matches, and the medium severity level to apply after 50 matches.

**Table 13-4** Rule severity levels

Rule severity level	Description
High	If a condition match occurs, it is labeled "High" severity.
Medium	If a condition match occurs, it is labeled "Medium" severity.
Low	If a condition match occurs, it is labeled "Low" severity.
Info	If a condition match occurs, it is labeled "Info" severity.

## Policy authoring privileges

Policy authors configure and manage policies and their rules and exceptions. To author policies, a user must be assigned to a role that grants the policy authoring privilege. This role can be expanded to include management of policy groups, scanning targets, and credentials.

Response rule authoring privileges are separate credentials from policy authoring and administration privileges. Whether or not policy authors have response rule authoring privileges is based on your enterprise needs.

Table 13-5 describes the typical privileges for the policy and response rule authoring roles.

**Table 13-5** Policy authoring privileges

Role privilege	Description
Author Policies	Add, configure, and manage policies.
	Add, configure, and manage policy rules and exceptions.
	Import and export policy templates.
	Modify system-defined data identifiers and create custom data identifiers.
	Add, configure, and manage User Groups.
	Add response rules to policies (but do not create response rules).
	See "About role-based access control" on page 84.

**Table 13-5** Policy authoring privileges (continued)

Role privilege	Description
Enforce Server Administration	Add, configure, and manage policy groups.  Add, configure, and manage Data Profiles.
	See "Configuring roles" on page 91.
Author Response Rules	Add, configure, and manage response rules (but do not add them to policies).  See "About response rule authoring privileges" on page 885.

#### **Data Profiles**

Data Profiles are user-defined configurations that you create to implement Exact Data Matching (EDM), Indexed Document Matching (IDM), and Vector Machine Learning (VML) policy conditions.

See "Data Loss Prevention policy detection technologies" on page 298.

Table 13-6 describes the types of Data Profiles that the system supports.

**Table 13-6** Types of Data Profiles

Data Profile type	Description
Exact Data Profile	An Exact Data Profile is used for Exact Data Matching (EDM) policies. The Exact Data Profile contains data that has been indexed from a structured data source, such as a database, directory server, or CSV file. The Exact Data Profile runs on the detection server. If an EDM policy is deployed to an endpoint, the DLP Agent sends the message to the detection server for evaluation (two-tier detection).
	See "About the Exact Data Profile and index" on page 371.
	See "Introducing profiled Directory Group Matching (DGM)" on page 661.
	See "About two-tier detection for EDM on the endpoint" on page 377.
Indexed Document Profile	An Indexed Document Profile is used for Indexed Document Matching (IDM) policies. The Indexed Document Profile contains data that has been indexed from a collection of confidential documents. The Indexed Document Profile runs on the detection server. If an IDM policy is deployed to an endpoint, the DLP Agent sends the message to the detection server for evaluation (two-tier detection).
	See "About the Indexed Document Profile" on page 465.
	See "About the indexing process" on page 466.

**		
Data Profile type	Description	
Vector Machine Learning Profile	A Vector Machine Learning Profile is used for Vector Machine Learning (VML) policies. The Vector Machine Learning Profile contains a statistical model of the features (keywords) extracted from content that you want to protect. The VML profile is loaded into memory by the detection server and DLP Agent. VML does not require two-tier detection.	
	See "About the Vector Machine Learning Profile" on page 510.	
	See "Configuring VML profiles and policy conditions" on page 513.	

Types of Data Profiles (continued) **Table 13-6** 

## **User Groups**

You define User Groups on the Enforce Server. User Groups contain user identity information that you populate by synchronizing the Enforce Server with a group directory server (Microsoft Active Directory).

You must have at least policy authoring or server administrator privileges to define User Groups. You must define the User Groups before you synchronize users.

Once you define a User Group, you populate it with users, groups, and business units from your directory server. After the user group is populated, you associate it with the User/Sender and Recipient detection rules or exceptions. The policy only applies to members of that User Group

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

See "Configuring directory server connections" on page 127.

See "Configuring User Groups" on page 654.

## Policy import and export

You can export and import policy templates to and from the Enforce Server. This feature lets you share policies across environments, version existing policies, and archive legacy policies.

Consider a scenario where you author and refine a policy on a test system and then export the policy as a template. You then import this policy to a production system for deployment to one or more detection servers. Or, if you want to retire a policy, you export it as a template for archiving, then remove it from the system.

See "Importing policy templates" on page 349.

See "Exporting policy detection as a template" on page 350.

A policy template is an XML file. The template contains the policy metadata, and the detection and the group rules and exceptions. If a policy template contains more than one condition that requires a Data Profile, the system imports only one of these conditions. A policy template does not include policy response rules, or modified or custom data identifiers.

Table 13-7 describes policy template components.

**Table 13-7** Components included in policy templates

Policy component	Description	Included in Template
Policy metadata (name, description, label)	The name of the template has to be less than 60 characters or it does not appear in the <b>Imported Templates</b> list.	YES
Described Content Matching (DCM) rules and exceptions	If the template contains only DCM methods, it imports as exported without changes.	YES
Exact Data Matching (EDM) and Indexed Document Matching (IDM) conditions	If the template contains multiple EDM or IDM match conditions, only one is exported.  If the template contains an EDM and an IDM condition, the system drops the IDM.	YES
User Group	User group methods are maintained on import only if the user groups exist on the target before import.	NO
Policy Group	Policy groups do not export. On import you can select a local policy group, otherwise the system assigns the policy to the Default Policy group.	NO
Response Rules	You must define and add response rules to policies from the local Enforce Server instance.	NO
Data Profiles	On import you must reference a locally defined Data Profile, otherwise the system drops any methods that require a Data Profile.	NO
Custom data identifiers	Modified and custom data identifiers do not export.	NO
Custom protocols	Custom protocols do not export.	NO
Policy state	Policy state (Active/Suspended) does not export.	NO

## **Workflow for implementing policies**

Policies define the content, event context, and identities you want to detect. Policies may also define response rule actions if a policy is violated. Successful policy

creation is a process that requires careful analysis and proper configuration to achieve optimum results.

Table 13-8 describes the typical workflow for implementing Data Loss Prevention policies.

Policy implementation process **Table 13-8** 

Action	Description
Familiarize yourself with the different types of detection technologies and methods that Symantec Data Loss Prevention provides, and considerations for authoring data loss prevention policies.	See "Detecting data loss" on page 296.  See "Data Loss Prevention policy detection technologies" on page 298.  See "Policy matching conditions" on page 300.  See "Best practices for authoring policies" on page 357.
Develop a policy detection strategy that defines the type of data you want to protect from data loss.	See "Develop a policy strategy that supports your data security objectives" on page 359.
Review the policy templates that ship with Symantec Data Loss Prevention, and any templates that you import manually or by solution pack.	See "Policy templates" on page 286. See "Solution packs" on page 287.
Create policy groups to control how your policies are accessed, edited, and deployed.	See "Policy groups" on page 287. See "Policy deployment" on page 288.
To detect exact data or content or similar unstructured data, create one or more Data Profiles.	See "Data Profiles" on page 291.
To detect exact identities from a synchronized directory server (Active Directory), configure one or more User Groups.	See "User Groups" on page 292.
Configure conditions for detection and group rules and exceptions.	See "Creating a policy from a template" on page 312.
Test and tune your policies.	See "Test and tune policies to improve match accuracy" on page 361.
Add response rules to the policy to take action when the policy is violated.	See "About response rules" on page 875.
Manage the policies in your enterprise.	See "Manage and add policies" on page 345.

## Viewing, printing, and downloading policy details

You may be required to share high-level details about your policies with individuals who are not Symantec Data Loss Prevention users. For example, you might be asked to provide policy details to an information security officer in your company. or to and outside security auditor. To facilitate such an action, you can view and print policy details in an easily readable format from the Policy List screen. The policy detail view does not include any technical nomenclature or branding specific to Symantec Data Loss Prevention. It displays the policy name, description, label, group, status, version, and last modified date for the policy. It also displays the detection and the response rules for that policy.

Any user with the Author Policies privilege for a given policy or set of policies can view and print policy details.

See "Policy authoring privileges" on page 290.

Table 13-9 describes how to work with policy details.

**Table 13-9** Working with policy details

Action	Description
View and print details for a single policy.	See "Viewing and printing policy details" on page 352.
Download details for all policies.	See "Downloading policy details" on page 353.

## Overview of policy detection

This chapter includes the following topics:

- Detecting data loss
- Data Loss Prevention policy detection technologies
- Policy matching conditions
- Detection messages and message components
- Exception conditions
- Compound conditions
- Policy detection execution
- Two-tier detection for DLP Agents

## **Detecting data loss**

Symantec Data Loss Prevention detects data from virtually any type of message or file, any user, sender, or recipient, wherever your data or endpoints exist. You can use Data Loss Prevention to detect both the content and the context of data within your enterprise. You define and manage your detection policies from the centralized, Web-based Enforce Server administration console.

See "Content that can be detected" on page 297.

See "Files that can be detected" on page 297.

See "Protocols that can be monitored" on page 297.

See "Endpoint events that can be detected" on page 298.

See "Identities that can be detected" on page 298.

See "Languages that can be detected" on page 298.

#### Content that can be detected

Symantec Data Loss Prevention detects data and document content, including text, markup, presentations, spreadsheets, archive files and their contents, email messages, database files, designs and graphics, multimedia files, and more. For example, the system can open a compressed file and scan a Microsoft Word document within the compressed file for the keyword "confidential." If the keyword is matched, the detection engine flags the message as an incident.

Content-based detection is based on actual content, not the file itself. A detection server can detect extracts or derivatives of protected or described content. This content may include sections of documents that have been copied and pasted to other documents or emails. A detection server can also identify sensitive data in a different file format than the source file. For example, if a confidential Word file is fingerprinted, the detection engine can match the content emailed in a PDF attachment.

See "Content matching conditions" on page 301.

#### Files that can be detected

Symantec Data Loss Prevention recognizes many types of files and attachments based on their context, including file type, file name, and file size. Symantec Data Loss Prevention identifies over 300 types of files, including word-processing formats, multimedia files, spreadsheets, presentations, pictures, encapsulation formats, encryption formats, and others.

For file type detection, the system does not rely on the file extension to identify the file type. For example, the system recognizes a Microsoft Word file even if a user changes the file extension to .txt. In this case the detection engine checks the binary signature of the file to match its type.

See "File property matching conditions" on page 302.

#### Protocols that can be monitored

Symantec Data Loss Prevention detects messages on the network by identifying the protocol signature: email (SMTP), Web (HTTP), file transfer (FTP), newsgroups (NNTP), TCP, Telnet, and SSL.

You can configure a detection server to listen on non-default ports for data loss violations. For example, if your network transmits Web traffic on port 81 instead of port 80, the system still recognizes the transmitted content as HTTP.

See "Protocol matching condition for network and mobile" on page 303.

#### Endpoint events that can be detected

Symantec Data Loss Prevention lets you detect data loss violations at several endpoint destinations. These destinations include the local drive, CD/DVD drive, removable storage devices, network file shares, Windows Clipboard, printers and faxes, and application files. You can also detect protocol events on the endpoint for email (SMTP), Web (HTTP), and file transfer (FTP) traffic.

For example, the DLP Agent (installed on each endpoint computer) can detect the copying of a confidential file to a USB device. Or, the DLP Agent can allow the copying of files only to a specific class of USB device that meets corporate encryption requirements.

See "Endpoint matching conditions" on page 304.

#### Identities that can be detected

Symantec Data Loss Prevention lets you detect the identity of data users, message senders, and message recipients using a variety of methods. These methods include described identity patterns and exact identities matched from a directory server or a corporate database.

For example, you can detect email messages sent by a specific user, or allow email messages sent to or from a specific group of users as defined in your Microsoft Active Directory server

See "Groups (identity) matching conditions" on page 304.

#### Languages that can be detected

Symantec Data Loss Prevention provides broad international support for detecting data loss in many languages. Supported languages include most Western and Central European languages, Hebrew, Arabic, Chinese (simplified and traditional), Japanese, Korean, and more.

The detection engine uses Unicode internally. You can build localized policy rules and exceptions using any detection technology in any supported language.

See "Supported languages for detection" on page 65.

See "Detecting non-English language content" on page 604.

## Data Loss Prevention policy detection technologies

Symantec Data Loss Prevention provides several types of detection technologies to help you author policies to detect data loss. Each type of detection technology provides unique capabilities. Often you combine technologies in policies to achieve

precise detection results. In addition, Symantec Data Loss Prevention provides you with several ways to extend policy detection and match any type of data, content, or files you want.

See "About Data Loss Prevention policies" on page 283.

See "Best practices for authoring policies" on page 357.

Table 14-1 lists the various types of the detection technologies and customizations provided by Data Loss Prevention.

**Table 14-1** Data Loss Prevention detection technologies

Table 14-1 Data Loss Frevention detection technologies		
Technology	Description	
Exact Data Matching (EDM)	Use EDM to detect personally identifiable information.	
	See "Introducing Exact Data Matching (EDM)" on page 367.	
Indexed Document Matching	Use IDM to detect exact files and file contents, and derivative content.	
(IDM)	See "Introducing Indexed Document Matching (IDM)" on page 462.	
Vector Machine Learning	Use VML to detect similar document content.	
(VML)	See "Introducing Vector Machine Learning (VML)" on page 509.	
Directory Group Matching (DGM)	Use DGM to detect exact identities synchronized from a directory server or profiled from a database.	
	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.	
	See "Introducing profiled Directory Group Matching (DGM)" on page 661.	
Described Content Matching	Use DCM to detect message content and context, including:	
(DCM)	■ Data Identifiers to match content using precise patterns and data validators.	
	See "Introducing data identifiers" on page 541.  Keywords to detect content using key words, key phrases, and keyword dictionaries.	
	See "Introducing keyword matching" on page 584.	
	Regular Expressions to detect characters, patterns, and strings.	
	See "Introducing regular expression matching" on page 598.	
	<ul> <li>File properties to detect files by type, name, size, and custom type.</li> <li>See "Introducing file property detection" on page 609.</li> </ul>	
	<ul> <li>User, sender, and recipient patterns to detect described identities.</li> </ul>	
	See "Introducing described identity matching" on page 643.	
	■ Protocol signatures to detect network and mobile traffic.	
	See "Introducing protocol monitoring for network" on page 626.	
	See "Introducing protocol monitoring for mobile" on page 627.  Destinations, devices, and protocols to detect endpoint events.	
	See "Introducing endpoint event detection" on page 632.	

**Table 14-1** Data Loss Prevention detection technologies (continued)

Technology	Description
Custom policy detection methods	Data Loss Prevention provides methods for customizing and extending detection, including:
	<ul> <li>Custom Data Identifiers         Implement your own data identifier patterns and system-defined validators.     </li> <li>See "Introducing data identifiers" on page 541.</li> <li>Custom script validators for Data Identifiers         Use the Symantec Data Loss Prevention Scripting Language to validate custom data types.     </li> <li>See "Workflow for creating custom data identifiers" on page 570.</li> <li>Custom file type identification         Use the Symantec Data Loss Prevention Scripting Language to detect custom file types.     </li> <li>See "About custom file type identification" on page 610.</li> <li>Custom endpoint device detection         Detect or allow any endpoint device using regular expressions.     </li> <li>See "About endpoint device detection" on page 634.</li> <li>Custom network protocol detection         Define custom TCP ports to tap.     </li> <li>See "Introducing protocol monitoring for network" on page 626.</li> <li>Custom content extraction         Use a plug-in to identify custom file formats and extract file contents for analysis by the detection server.     </li> <li>See "Overview of detection file format support" on page 667.</li> </ul>
	or over the district me termet support on page cor.

## **Policy matching conditions**

Symantec Data Loss Prevention provides several types of match conditions, each offering unique detection capabilities. You implement match conditions in policies as rules or exceptions. Detection rules use conditions to match message content or context. Group rules use conditions to match identities. You can also use conditions as detection and group policy exceptions.

See "Exception conditions" on page 307.

Table 14-2 lists the various types of policy matching conditions provided by Data Loss Prevention.

Condition type	Description
Content	See "Content matching conditions" on page 301.
File property	See "File property matching conditions" on page 302.
Protocol	See "Protocol matching condition for network and mobile" on page 303.
Endpoint	See "Endpoint matching conditions" on page 304.
Groups (identity)	See "Groups (identity) matching conditions" on page 304.

**Table 14-2** Policy match condition types

#### Content matching conditions

Symantec Data Loss Prevention provides several conditions to match message content. Certain content conditions require an associated Data Profile and index. For content detection, you can match on individual message components, including header, body, attachments, and subject for some conditions.

See "Detection messages and message components" on page 305.

See "Content that can be detected" on page 297.

Table 14-3 lists the content matching conditions that you can use without a Data Profile and index.

Content matching conditions **Table 14-3** 

Content rule type	Description
Content Matches Regular Expression	Match described content using regular expressions.  See "Introducing regular expression matching" on page 598.  See "Configuring the Content Matches Regular Expression condition" on page 600.
Content Matches Keyword	Match described content using keywords, key phrases, and keyword dictionaries  See "Introducing keyword matching" on page 584.  See "Configuring the Content Matches Keyword condition" on page 591.
Content Matches Data Identifier	Match described content using Data Identifier patterns and validators.  See "Introducing data identifiers" on page 541.  See "Configuring the Content Matches data identifier condition" on page 552.

Table 14-4 lists the content matching conditions that require a Data Profile and index.

See "Data Profiles" on page 291.

See "Two-tier detection for DLP Agents" on page 309.

**Table 14-4** Index-based content matching conditions

Content rule type	Description
Content Matches Exact Data From an Exact Data Profile	Match exact data profiled from a structured data source such as a database or CSV file.
(EDM)	See "Introducing Exact Data Matching (EDM)" on page 367.
	See "Configuring the Content Matches Exact Data policy condition" on page 396.
	<b>Note:</b> This condition requires two-tier detection on the endpoint. See "About two-tier detection for EDM on the endpoint" on page 377.
Content Matches Document	Match files and file contents exactly or partially using fingerprinting
Signature From an Indexed Document Profile (IDM)	See "Introducing Indexed Document Matching (IDM)" on page 462.
Document Profile (IDM)	See "Configuring the Content Matches Document Signature policy condition" on page 497.
	<b>Note:</b> This condition requires two-tier detection on the endpoint. See "About the Indexed Document Profile" on page 465.
Detect using Vector Machine	Match file contents with features similar to example content you have trained.
Learning profile (VML)	See "Introducing Vector Machine Learning (VML)" on page 509.
	See "Configuring the Detect using Vector Machine Learning Profile condition" on page 525.

### File property matching conditions

Symantec Data Loss Prevention provides several conditions to match file properties, including file type, file size, and file name.

See "Files that can be detected" on page 297.

**Table 14-5** File property match conditions

Condition type	Description	
Message Attachment or File Type Match	Match specific file formats and document attachments.	
туре максп	See "About file type matching" on page 609.	
	See "Configuring the Message Attachment or File Type Match condition" on page 612.	

**Table 14-5** File property match conditions (continued)

Condition type	Description		
Message Attachment or File	Match files or attachments over or under a specified size.		
Size Match	See "About file size matching" on page 611.		
	See "Configuring the Message Attachment or File Size Match condition" on page 613.		
Message Attachment or File	Match files or attachments that have a specific name or match wildcards.		
Name Match	See "About file name matching" on page 611.		
	See "Configuring the Message Attachment or File Name Match condition" on page 614.		
Message/Email Properties and Attributes	Classify Microsoft Exchange email messages based on specific message attributes (MAPI attributes).		
	See "Configuring the Message/Email Properties and Attributes condition" on page 623.		
	<b>Note:</b> This condition is available for use with Data Classification for Enterprise Vault. See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> .		
Custom File Type Signature	Match custom file types based on their binary signature using scripting.		
	See "About custom file type identification" on page 610.		
	See "Enabling the Custom File Type Signature condition in the policy console" on page 616.		

## Protocol matching condition for network and mobile

Symantec Data Loss Prevention provides the single **Protocol Monitoring** condition to match network and mobile traffic for policy detection rules and exceptions.

See "Protocols that can be monitored" on page 297.

**Table 14-6** Protocol matching condition for network and mobile monitoring

Match condition	Description			
Protocol Monitoring	Match incidents on the network transmitted using a specified protocol, including SMTP, FTP, HTTP/S, IM, and NNTP.			
	See "Introducing protocol monitoring for network" on page 626.			
	See "Configuring the Protocol Monitoring condition for network detection" on page 628.			
	Match incidents sent to and from mobile devices over the HTTP/S and FTP protocols.			
	See "Introducing protocol monitoring for mobile" on page 627.			
	See "Configuring the Protocol Monitoring condition for mobile detection" on page 629.			

#### **Endpoint matching conditions**

Symantec Data Loss Prevention provides several conditions for matching endpoint events.

See "Endpoint events that can be detected" on page 298.

**Table 14-7 Endpoint matching conditions** 

Condition	Description			
Protocol or Endpoint Monitoring	Match endpoint messages transmitted using a specified transport protocol or when data is moved or copied to a particular destination.			
	See "Introducing endpoint event detection" on page 632.			
	See "Configuring the Endpoint Monitoring condition" on page 635.			
Endpoint Device Class or ID	Match endpoint events occurring on specified hardware devices.			
	See "Introducing endpoint event detection" on page 632.			
	See "Configuring the Endpoint Device Class or ID condition" on page 638.			
Endpoint Location	Match endpoint events depending if the DLP Agent is on or off the corporate network.			
	See "Introducing endpoint event detection" on page 632.			
	See "Configuring the Endpoint Location condition" on page 637.			

#### Groups (identity) matching conditions

Symantec Data Loss Prevention provides several conditions for matching the identity of users and groups, and message senders and recipients.

The sender and recipient pattern rules are reusable across policies. The Directory Group Matching (DGM) rules let you match on sender and recipients derived from Active Directory (synchronized DGM) or from an Exact Data Profile (profiled DGM).

See "Identities that can be detected" on page 298.

See "Two-tier detection for DLP Agents" on page 309.

Available group rules for identity matching **Table 14-8** 

Group rule	Description	
Sender/User Matches Pattern	Match message senders and users by email address, user ID, IM screen name, and IP address.	
	See "Introducing described identity matching" on page 643.	
	See "Configuring the Sender/User Matches Pattern condition" on page 645.	

**Table 14-8** Available group rules for identity matching (continued)

Group rule	Description			
Recipient Matches Pattern	Match message recipients by email or IP address, or Web domain.			
	See "Introducing described identity matching" on page 643.			
	See "Configuring the Recipient Matches Pattern condition" on page 648.			
Sender/User based on a	Match message senders and users from a synchronized directory server.			
Directory Server Group	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.			
	See "Configuring the Sender/User based on a Directory Server Group condition" on page 657.			
Sender/User based on a	Match message senders and users from a profiled directory server.			
<b>Directory from:</b> an Exact Data Profile	See "Introducing profiled Directory Group Matching (DGM)" on page 661.			
Trome	See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.			
	<b>Note:</b> This condition requires two-tier detection on the endpoint. See "About two-tier detection for profiled DGM" on page 661.			
Recipient based on a Directory	Match message recipients from a synchronized directory server.			
Server Group	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.			
	See "Configuring the Recipient based on a Directory Server Group condition" on page 658.			
	<b>Note:</b> This condition requires two-tier detection on the endpoint. See "About two-tier detection for synchronized DGM" on page 654.			
Recipient based on a Directory	Match message recipients from a profiled directory server.			
from: an Exact Data Profile	See "Configuring Exact Data profiles for DGM" on page 662.			
	See "Configuring the Recipient based on a Profiled Directory condition" on page 664.			
	<b>Note:</b> This condition requires two-tier detection on the endpoint. See "About two-tier detection for profiled DGM" on page 661.			

## **Detection messages and message components**

Data Loss Prevention detection servers and DLP Agents receive input data for analysis in the form of messages. The system determines the message type; for example, an email or a Word document. Depending on the message type, the system either parses the message content into components (header, subject, body, attachments), or it leaves the message intact. The system evaluates the message or message components to see if any policy match conditions apply. If a condition applies and it supports component matching, the system evaluates the content against each selected message component. If the condition does not support component matching, the system evaluates the entire message against the match condition.

See "Selecting components to match on" on page 336.

The content-based conditions support cross-component matching. You can configure the DCM content conditions to match across all message components. The EDM condition matches on message envelope, body, and attachments. The document conditions match on the message body and attachments, except File Type and Name which only match on the attachment. Protocol, endpoint, and identity conditions match on the entire message, as does any condition evaluated by the DLP Agent. The subject component only applies to SMTP email or NNTP messages, and Data Classification.

See "About matching on the message Subject for Data Classification Services" on page 621.

Table 14-9 summarizes the component matching supported by each match condition type.

Table 14-9	Message components to match on
------------	--------------------------------

Condition type	Envelope	Subject	Body	Attachment(s)
Described content (DCM) conditions for content detection:	match	match	match	match
Keyword, Data Identifier, Regular Expression				
Exact Data Matching (EDM)	match		match	match
Indexed Document Matching (IDM)			match	match
Vector Machine Learning (VML)			match	match
File Size (DCM)			match	match
File Type and File Name (DCM)				match
Protocol (DCM)	match (entire message)			
Endpoint (DCM)	match (entire message)			
Identity (DCM and DGM)	match (entire message)			

**Table 14-9** Message components to match on (continued)

Condition type	Envelope	Subject	Body	Attachment(s)
Any condition evaluated by the DLP Agent		match (ent	tire message)	

## **Exception conditions**

Symantec Data Loss Prevention provides policy exceptions to exclude messages and message components from matching. You can use exception conditions to refine the scope of your detection and group rules.

See "Use a limited number of exceptions to narrow detection scope" on page 363.

Warning: Do not use multiple compound exceptions in a single policy. Doing so can cause detection to run out of memory. If you find that the policy needs multiple compound exceptions to produce matches, you should reconsider the design of the matching conditions.

The system evaluates an inbound message or message component against policy exceptions before policy rules. If the exception supports cross-component matching (content-based exceptions), the exception can be configured to match on individual message components. Otherwise, the exception matches on the entire message.

If an exception is met, the system ejects the entire message or message component containing the content that triggered the exception. The ejected message or message component is no longer available for evaluation against policy rules. The system does not discard only the matched content or data item; it discards the entire message or message component that contained the excepted item.

Note: Symantec Data Loss Prevention does not support match-level exceptions, only component or message-level exceptions.

For example, consider a policy that has a detection rule with one condition and an exception with one condition. The rule matches messages containing Microsoft Word attachments and generates an incident for each match. The exception excludes from matching messages from ceo@company.com. An email from ceo@company.com that contains a Word attachment is excepted from matching and does not trigger an incident. The detection exception condition excluding ceo@company.com messages takes precedence over the detection rule match condition that would otherwise match on the message.

See "Policy detection execution" on page 308.

You can implement any condition as an exception, except the EDM condition Content Matches Exact Data From. In addition, Network Prevent for Web does not support synchronized DGM exceptions. You can implement IDM as an exception, but the exception excludes exact files from matching, not file contents. To exclude file contents, you "whitelist" it. VML can be used as an exception if the content is from the same category.

See "Adding an exception to a policy" on page 337.

See "CAN-SPAM Act policy template" on page 805.

See "Whitelisting file contents to exclude from partial matching" on page 476.

## Compound conditions

A valid policy must declare at least one rule that defines at least one match condition. The condition matches input data to detect data loss. A rule with a single condition is a simple rule. Optionally, you can declare multiple conditions within a single detection or group rule. A rule with multiple conditions is a compound condition.

For compound conditions, each condition in the rule must match to trigger a violation. Thus, for a single policy that declares one rule with two conditions, if one condition matches but the other does not, detection does not report a match. If both conditions match, detection reports a match, assuming that the rule is set to count all matches. In programmatic terms, two or more conditions in the same rule are ANDed together.

Like rules, you can declare multiple conditions within a single exception. In this case, all conditions in the exception must match for the exception to apply.

See "Policy detection execution" on page 308.

See "Use compound conditions to improve match accuracy" on page 363.

See "Exception conditions" on page 307.

## Policy detection execution

You can include any combination of detection rules, group rules, and exceptions in a single policy. A detection server evaluates policy exceptions first. If any exception is met, the entire message or message component matching the exception is ejected and is no longer available for policy matching.

The detection server evaluates the detection and group rules in the policy on a per-rule basis. In programmatic terms, where you have a single policy definition, the connection between conditions in the same rule or exception is AND (compound conditions). The connection between two or more rules of the same type is OR (for example, 2 detection rules). But, if you combine rules of different type in a single policy (for example, 1 detection rule and 1 group rule), the connection between the rules is AND. In this configuration both rules must match to trigger an incident. However, exception conditions created across the "Detection" and "Groups" tabs are connected by an implicit OR.

See "Compound conditions" on page 308.

See "Exception conditions" on page 307.

Table 14-10 summarizes the policy condition execution logic for the detection server for various policy configurations.

Policy configuration	Logic	Description
Compound conditions	AND	If a single rule or exception in a policy contains two or more match conditions, all conditions must match.
Rules or exceptions of same type	OR	If there are two detection rules in a single policy, or two group rules in a single policy, or two exceptions of the same type (detection or group), the rules or exceptions are independent of each other.
Rules of different type	AND	If one or more detection rules is combined with one or more group rules in a single policy, the rules are dependent.
Exceptions of different type	OR	If one or more detection exceptions is combined with one or more group exceptions in a single policy, the exceptions are independent.

Table 14-10 Policy condition execution logic

## Two-tier detection for DLP Agents

Symantec Data Loss Prevention uses a two-tier detection architecture to analyze activity on endpoints for some index-based match conditions.

Two-tier detection requires communication and data transfer between the DLP Agent and the Endpoint Server to detect incidents. If a match condition requires two-tier detection, the condition is not evaluated locally on the endpoint by the DLP Agent. Instead, the DLP Agent sends the data to the Endpoint Server for policy evaluation.

See "About policies for endpoints" on page 1365.

The effect of two-tier detection is that policy evaluation is delayed for the time it takes the data to be sent to and evaluated by the Endpoint Server. If the DLP Agent is not connected to the network or cannot communicate with the Endpoint Server.

the condition requiring two-tier detection is not evaluated until the DLP Agent connects. This delay can impact performance of the DLP Agent if the message is a large file or attachment.

See "Troubleshooting policies" on page 353.

Two-tier detection has implications for the kinds of policies you author for endpoints. You can reduce the potential bottleneck of two-tier detection by being aware of the detection conditions that require two-tier detection and author your endpoint policies in such a way to eliminate or reduce the need for two-tier detection.

See "Author policies to limit the potential effect of two-tier detection" on page 364.

Table 14-11 lists the detection conditions that require two-tier detection on the endpoint.

Note: You cannot combine an Endpoint Prevent: Notify or Block response rule with two-tier match conditions, including Exact Data Matching (EDM), Directory Group Matching (DGM), and Indexed Document Matching (IDM) when two-tier detection is enabled. If you do, the system displays a warning for both the detection condition and the response rule.

Table 14-11 Policy matching conditions requiring two-tier detection

Detection technology	Match condition	Description
Exact Data Matching (EDM)	Content Matches Exact Data from an Exact Data Profile	See "Introducing Exact Data Matching (EDM)" on page 367.
		See "About two-tier detection for EDM on the endpoint" on page 377.
Profiled Directory Group Matching (DGM)	Sender/User based on a Directory from an Exact Data Profile	See "Introducing profiled Directory Group Matching (DGM)" on page 661.
	Recipient based on a Directory from an Exact Data Profile	See "About two-tier detection for profiled DGM" on page 661.
Synchronized Directory Group Matching (DGM)	Recipient based on a Directory Server Group	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.
		See "About two-tier detection for synchronized DGM" on page 654.

Policy matching conditions requiring two-tier detection (continued) Table 14-11

Detection technology	Match condition	Description
Indexed Document Matching (IDM)	Content Matches Document Signature from an Indexed Document Profile	See "Introducing Indexed Document Matching (IDM)" on page 462.  See "Two-tier IDM detection" on page 465.  Note: Two-tier detection for IDM only applies if it is enabled on the Endpoint Server (two_tier_idm = on). If Endpoint IDM is enabled (two_tier_idm = off), two-tier detection is not used.

# Creating policies from templates

This chapter includes the following topics:

- Creating a policy from a template
- US Regulatory Enforcement policy templates
- UK and International Regulatory Enforcement policy templates
- Customer and Employee Data Protection policy templates
- Confidential or Classified Data Protection policy templates
- Network Security Enforcement policy templates
- Acceptable Use Enforcement policy templates
- Choosing an Exact Data Profile
- Choosing an Indexed Document Profile

## Creating a policy from a template

You can create a policy from a system-provided template or from a template you import to the Enforce Server.

See "Policy templates" on page 286.

See "Policy import and export" on page 292.

**Table 15-1** Create a policy from a template

Action	Description
Add a policy from a template.	See "Adding a new policy or policy template" on page 325.
Choose the template you want to use.	At the <b>Manage &gt; Policies &gt; Policy List &gt; New Policy - Template List</b> screen the system lists all policy templates.
	System-provided template categories:
	<ul> <li>See "US Regulatory Enforcement policy templates" on page 315.</li> <li>See "UK and International Regulatory Enforcement policy templates" on page 317.</li> <li>See "Customer and Employee Data Protection policy templates" on page 317.</li> <li>See "Confidential or Classified Data Protection policy templates" on page 319.</li> <li>See "Network Security Enforcement policy templates" on page 320.</li> <li>See "Acceptable Use Enforcement policy templates" on page 320.</li> </ul>
	Imported Templates appear individually after import:
	■ See "Importing policy templates" on page 349.
	<b>Note:</b> See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for information about Classification policy templates.
Click <b>Next</b> to configure the policy.	For example, select the <b>Webmail</b> policy template and click <b>Next</b> .
	See "Configuring policies" on page 326.
Choose a Data Profile (if prompted).	If the template relies on one or more Data Profiles, the system prompts you to select each:  Exact Data Profile See "Choosing an Exact Data Profile" on page 322.  Indexed Document Profile
	See "Choosing an Indexed Document Profile" on page 323.
	If you do not have a Data Profile, you can either:
	<ul> <li>Cancel the policy definition process, define the profile, and resume creating the policy from the template.</li> <li>Click Next to configure the policy.</li> <li>On creation of the policy, the system drops any rules or exceptions that rely on the Data Profile.</li> </ul>
	<b>Note:</b> You should use a profile if a template calls for it.

Create a policy from a template (continued) Table 15-1

Action	Description
Edit the policy name or description (optional).	If you intend to modify a system-defined template, you may want to change the name so you can distinguish it from the original.
	See "Configuring policies" on page 326.
	<b>Note:</b> If you want to export the policy as a template, the policy name must be less than 60 characters. If it is more, the template does not appear in the <b>Imported Templates</b> section of the <b>Template List</b> screen.
	<b>Note:</b> The <b>Policy Label</b> field is reserved for the Symantec Data Insight Self-Service Portal.
Select a policy group (if	If you have defined a policy group, select it from the <b>Policy Group</b> list.
necessary).	See "Creating and modifying policy groups" on page 348.
	If you have not defined a policy group, the system deploys the policy to the <b>Default Policy Group</b> .
Edit the policy rules or exceptions (if necessary).	The <b>Configure Policy</b> screen displays the rules and exceptions (if any) provided by the policy.
	You can modify, add, and remove policy rules and exceptions to meet your requirements.
	See "Configuring policy rules" on page 330.
	See "Configuring policy exceptions" on page 340.
Save the policy and export it	Click <b>Save</b> to save the policy.
(optional).	You can export policy detection as a template for sharing or archiving.
	See "Exporting policy detection as a template" on page 350.
	For example, if you changed the configuration of a system-defined policy template, you may want to export it for sharing across environments.
Test and tune the policy	Test and tune the policy using data the policy should and should not detect.
(recommended).	Review the incidents that the policy generates. Refine the policy rules and exceptions as necessary to reduce false positives and false negatives.
Add response rules (optional).	Add response rules to the policy to report and remediate violations.
	See "Implementing response rules" on page 886.
	<b>Note:</b> Response rules are not included in policy templates.

## **US Regulatory Enforcement policy templates**

Symantec Data Loss Prevention provides several policy templates supporting US Regulatory Enforcement guidelines.

US Regulatory Enforcement policy templates **Table 15-2** 

Policy template	Description
CAN-SPAM Act	Establishes requirements for sending commercial email.
	See "CAN-SPAM Act policy template" on page 805.
Defense Message System (DMS) GENSER	Detects information classified as confidential.
Classification	See "Defense Message System (DMS) GENSER Classification policy template" on page 813.
Export Administration Regulations (EAR)	Enforces the U.S. Department of Commerce Export Administration Regulations (EAR).
	See "Export Administration Regulations (EAR) policy template" on page 817.
FACTA 2003 (Red Flag Rules)	Enforces sections 114 and 315 (or Red Flag Rules) of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.
	See "FACTA 2003 (Red Flag Rules) policy template" on page 818.
Gramm-Leach-Bliley	This policy limits sharing of consumer information by financial institutions.
	See "Gramm-Leach-Bliley policy template" on page 824.
HIPAA and HITECH (including PHI)	This policy enforces the US Health Insurance Portability and Accountability Act (HIPAA).
	See "HIPAA and HITECH (including PHI) policy template" on page 826.
International Traffic in Arms Regulations (ITAR)	This policy enforces the US Department of State ITAR provisions.
	See "International Traffic in Arms Regulations (ITAR) policy template" on page 832.
NASD Rule 2711 and NYSE Rules 351 and 472	This policy protects the name(s) of any companies that are involved in an upcoming stock offering.
	See "NASD Rule 2711 and NYSE Rules 351 and 472 policy template" on page 835.

Table 15-2 US Regulatory Enforcement policy templates (continued)

Policy template	Description
NASD Rule 3010 and NYSE Rule 342	This policy monitors brokers-dealers communications.
	See "NASD Rule 3010 and NYSE Rule 342 policy template" on page 837.
NERC Security Guidelines for Electric Utilities	This policy detects the information that is outlined in the North American Electric Reliability Council (NERC) security guidelines for the electricity sector.
	See "NERC Security Guidelines for Electric Utilities policy template" on page 838.
Office of Foreign Assets Control (OFAC)	This template detects communications involving targeted OFAC groups.
	See "Office of Foreign Assets Control (OFAC) policy template" on page 841.
OMB Memo 06-16 and FIPS 199 Regulations	This template detects information that is classified as confidential.
	See "OMB Memo 06-16 and FIPS 199 Regulations policy template" on page 843.
Payment Card Industry Data Security Standard	This template detects Visa and MasterCard credit card number data.
	See "Payment Card Industry (PCI) Data Security Standard policy template" on page 845.
Sarbanes-Oxley	This template detects sensitive financial data.
	See "Sarbanes-Oxley policy template" on page 853.
SEC Fair Disclosure Regulation	This template detects data disclosure of material financial information.
	See "SEC Fair Disclosure Regulation policy template" on page 855.
State Data Privacy	This template detects breaches of state-mandated confidentiality.
	See "State Data Privacy policy template" on page 859.
US Intelligence Control Markings (CAPCO) and DCID 1/7	This template detects authorized terms to identify classified information in the US Federal Intelligence community.
	See "US Intelligence Control Markings (CAPCO) and DCID 1/7 policy template" on page 866.

## **UK and International Regulatory Enforcement policy** templates

Symantec Data Loss Prevention provides several policy templates for UK and International Regulatory Enforcement.

See "Creating a policy from a template" on page 312.

UK and International Regulatory Enforcement policy templates **Table 15-3** 

Policy template	Description
Caldicott Report	This policy protects UK patient information.
	See "Caldicott Report policy template" on page 802.
UK Data Protection Act 1998	This policy protects personal identifiable information.
	See "Data Protection Act 1998 (UK) policy template" on page 810.
EU Data Protection Directives	This policy detects personal data specific to the EU directives.
	See "Data Protection Directives (EU) policy template" on page 811.
Human Rights Act 1998	This policy enforces Article 8 of the act for UK citizens.
	See "Human Rights Act 1998 policy template" on page 830.
PIPEDA	This policy detects Canadian citizen customer data.
	See "PIPEDA policy template" on page 846.

## **Customer and Employee Data Protection policy** templates

Symantec Data Loss Prevention provides several policy templates for Customer and Employee Data Protection.

**Table 15-4** Customer and Employee Data Protection policy templates

Policy template	Description
Canadian Social Insurance Numbers	This policy detects patterns indicating Canadian social insurance numbers.
	See "Canadian Social Insurance Numbers policy template" on page 804.

Customer and Employee Data Protection policy templates **Table 15-4** (continued)

(continued)		
Policy template	Description	
Credit Card Numbers	This policy detects patterns indicating credit card numbers.	
	See "Credit Card Numbers policy template" on page 808.	
Customer Data Protection	This policy detects customer data.	
	See "Customer Data Protection policy template" on page 808.	
Employee Data Protection	This policy detects employee data.	
	See "Employee Data Protection policy template" on page 815.	
Individual Taxpayer Identification Numbers	This policy detects IRS-issued tax processing numbers.	
(ITIN)	See "Individual Taxpayer Identification Numbers (ITIN) policy template" on page 831.	
SWIFT Codes	This policy detects codes banks use to transfer money across international borders.	
	See "SWIFT Codes policy template" on page 862.	
UK Drivers License Numbers	This policy detects UK Drivers License Numbers.	
	See "UK Drivers License Numbers policy template" on page 863.	
UK Electoral Roll Numbers	This policy detects UK Electoral Roll Numbers.	
	See "UK Electoral Roll Numbers policy template" on page 864.	
UK National Insurance Numbers	This policy detects UK National Insurance Numbers.	
	See "UK National Insurance Numbers policy template" on page 864.	
UK National Health Service Number	This policy detects personal identification numbers issued by the NHS.	
	See "UK National Health Service (NHS) Number policy template" on page 864.	
UK Passport Numbers	This policy detects valid UK passports.	
	See "UK Passport Numbers policy template" on page 865.	
UK Tax ID Numbers	This policy detects UK Tax ID Numbers.	
	See "UK Tax ID Numbers policy template" on page 865.	
US Social Security Numbers	This policy detects patterns indicating social security numbers.	
	See "US Social Security Numbers policy template" on page 867.	

## **Confidential or Classified Data Protection policy** templates

Symantec Data Loss Prevention provides several policy templates for Confidential or Classified Data Protection.

**Table 15-5** Confidential or Classified Data Protection policy templates

Policy template	Description
Confidential Documents	This policy detects company-confidential documents.
	See "Confidential Documents policy template" on page 807.
Design Documents	This policy detects various types of design documents.
	See "Design Documents policy template" on page 814.
Encrypted Data	This policy detects the use of encryption by a variety of methods.
	See "Encrypted Data policy template" on page 817.
Financial Information	This policy detects financial data and information.
	See "Financial Information policy template" on page 822.
Merger and Acquisition Agreements	This policy detects information and communications about upcoming merger and acquisition activity.
	See "Merger and Acquisition Agreements policy template" on page 834.
Price Infomation	This policy detects specific SKU or pricing information.
	See "Price Information policy template" on page 848.
Project Data	This policy detects discussions of sensitive projects.
	See "Project Data policy template" on page 849.
Proprietary Media Files	This policy detects various types of video and audio files.
	See "Proprietary Media Files policy template" on page 849.
Publishing Documents	This policy detects various types of publishing documents.
	See "Publishing Documents policy template" on page 850.
Resumes	This policy detects active job searches.
	See "Resumes policy template" on page 852.

Policy template	Description
Source Code	This policy detects various types of source code.
	See "Source Code policy template" on page 858.
Symantec DLP Awareness and Avoidance	This policy detects any communications that refer to Symantec DLP or other data loss prevention systems and possible avoidance of detection.
	See "Symantec DLP Awareness and Avoidance policy template" on page 863.

**Table 15-5** Confidential or Classified Data Protection policy templates (continued)

## **Network Security Enforcement policy templates**

Symantec Data Loss Prevention provides several policy templates for Network Security Enforcement.

See "Creating a policy from a template" on page 312.

**Table 15-6** Network Security Enforcement policy templates

Policy template	Description
Common Spyware Upload Sites	This policy detects access to common spyware upload Web sites.
	See "Common Spyware Upload Sites policy template" on page 806.
Network Diagrams	This policy detects computer network diagrams.
	See "Network Diagrams policy template" on page 839.
Network Security	This policy detects evidence of hacking tools and attack planning.
	See "Network Security policy template" on page 840.
Password Files	This policy detects password file formats.
	See "Password Files policy template" on page 844.

## Acceptable Use Enforcement policy templates

Symantec Data Loss Prevention provides several policy templates for allowing acceptable uses of information.

Acceptable Use Enforcement policy templates **Table 15-7** 

Policy template	Description
Competitor Communications	This policy detects forbidden communications with competitors.
	See "Competitor Communications policy template" on page 806.
Forbidden Websites	This policy detects access to specified Web sites.
	See "Forbidden Websites policy template" on page 823.
Gambling	This policy detects any reference to gambling.
	See "Gambling policy template" on page 824.
Illegal Drugs	This policy detects conversations about illegal drugs and controlled substances.
	See "Illegal Drugs policy template" on page 831.
Media Files	This policy detects various types of video and audio files.
	See "Media Files policy template" on page 833.
Offensive Language	This policy detects the use of offensive language.
	See "Offensive Language policy template" on page 840.
Racist Language	This policy detects the use of racist language.
	See "Racist Language policy template" on page 851.
Restricted Files	This policy detects various file types that are generally inappropriate to send out of the company.
	See "Restricted Files policy template" on page 851.
Restricted Recipients	This policy detects communications with specified recipients.
	See "Restricted Recipients policy template" on page 851.
Sexually Explicit Language	This policy detects sexually explicit content.
	See "Sexually Explicit Language policy template" on page 857.
Violence and Weapons	This policy detects violent language and discussions about weapons.
	See "Violence and Weapons policy template" on page 867.
Webmail	This policy detects the use of a variety of Webmail services.
	See "Webmail policy template" on page 868.
Yahoo Message Board Activity	This policy detects Yahoo message board activity.
	See "Yahoo Message Board Activity policy template" on page 869.

Policy template	Description
Yahoo and MSN Messengers on Port 80	This policy detects Yahoo IM and MSN Messenger activity.
	See "Yahoo and MSN Messengers on Port 80 policy template" on page 870.

Table 15-7 Acceptable Use Enforcement policy templates (continued)

## Choosing an Exact Data Profile

If the policy template you select implements Exact Data Matching (EDM), the system prompts you to choose an Exact Data Profile. Table 15-8 lists the policy templates that are based on Exact Data Profiles.

If you do not have an Exact Data Profile, you can cancel policy creation and define a profile. Or, you can choose not to use an Exact Data Profile. In this case the system disables the associated EDM detection rules in the policy template. You can use any DCM rules or exceptions the policy template provides.

See "Introducing Exact Data Matching (EDM)" on page 367.

See "About the Exact Data Profile and index" on page 371.

#### To choose an Exact Data Profile

- Select an **Exact Data Profile** from the list of available profiles.
- Click **Next** to continue with creating the policy from the template.

Click **Previous** to return to the list of policy templates.

See "Creating a policy from a template" on page 312.

Note: When the system prompts you to select an Exact Data Profile, the display lists the data columns to include in the profile to provide the highest level of accuracy. If data fields in your Exact Data Profile are not represented in the selected policy template, the system displays those fields for content matching when you define the detection rule

Policy template	Description
Caldicott Report	See "Caldicott Report policy template" on page 802.
Customer Data Protection	See "Customer Data Protection policy template" on page 808.
Data Protection Act 1988	See "Data Protection Act 1998 (UK) policy template" on page 810.

Table 15-8 Policy templates that implement Exact Data Matching (FDM)

Table 15-8	Policy templates that implement Exact Data Matching (EDM)
	(continued)

Policy template	Description
Employee Data Protection	See "Employee Data Protection policy template" on page 815.
EU Data Protection Directives	See "Data Protection Directives (EU) policy template" on page 811.
Export Administration Regulations (EAR)	See "Export Administration Regulations (EAR) policy template" on page 817.
FACTA 2003 (Red Flag Rules)	See "FACTA 2003 (Red Flag Rules) policy template" on page 818.
Gramm-Leach-Bliley	See "Gramm-Leach-Bliley policy template" on page 824.
HIPAA and HITECK (including PHI)	See "HIPAA and HITECH (including PHI) policy template" on page 826.
Human Rights Act 1998	See "Human Rights Act 1998 policy template" on page 830.
International Traffic in Arms Regulations (ITAR)	See "International Traffic in Arms Regulations (ITAR) policy template" on page 832.
Payment Card Industry Data Security Standard	See "Payment Card Industry (PCI) Data Security Standard policy template" on page 845.
PIPEDA	See "PIPEDA policy template" on page 846.
Price Information	See "Price Information policy template" on page 848.
Resumes	See "Resumes policy template" on page 852.
State Data Privacy	See "SEC Fair Disclosure Regulation policy template" on page 855.

## **Choosing an Indexed Document Profile**

If the policy template you chose uses Indexed Document Matching (IDM) detection, the system prompts you to select the Document Profile.

See "Introducing Indexed Document Matching (IDM)" on page 462.

#### To use a Document Profile

- Select the **Document Profile** from the list of available profiles.
- Click **Next** to create the policy from the template.

See "Creating a policy from a template" on page 312.

If you do not have a Document Profile, you can cancel policy creation and define the Document Profile. Or, you can choose to not use a Document Profile. In this

case the system disables any IDM rules or exceptions for the policy instance. If the policy template contains DCM rules or exceptions, you may use them.

See "About the Indexed Document Profile" on page 465.

Policy templates that implement Indexed Document Matching (IDM) **Table 15-9** 

Policy template	Description	
CAN-SPAM Act (IDM exception)	See "CAN-SPAM Act policy template" on page 805.	
NASD Rule 2711 and NYSE Rules 351 and 472	See "NASD Rule 2711 and NYSE Rules 351 and 472 policy template" on page 835.	
NERC Security Guidelines for Electric Utilities	See "NERC Security Guidelines for Electric Utilities policy template" on page 838.	
Sarbanes-Oxley	See "Sarbanes-Oxley policy template" on page 853.	
SEC Fair Disclosure Regulation	See "SEC Fair Disclosure Regulation policy template" on page 855.	
Confidential Documents	See "Confidential Documents policy template" on page 807.	
Design Documents	See "Design Documents policy template" on page 814.	
Financial Information	See "Financial Information policy template" on page 822.	
Project Data	See "Project Data policy template" on page 849.	
Proprietary Media Files	See "Proprietary Media Files policy template" on page 849.	
Publishing Documents	See "Publishing Documents policy template" on page 850.	
Source Code	See "Source Code policy template" on page 858.	
Network Diagrams	See "Network Diagrams policy template" on page 839.	

# Configuring policies

This chapter includes the following topics:

- Adding a new policy or policy template
- Configuring policies
- Adding a rule to a policy
- Configuring policy rules
- Defining rule severity
- Configuring match counting
- Selecting components to match on
- Adding an exception to a policy
- Configuring policy exceptions
- Configuring compound match conditions
- Input character limits for policy configuration

## Adding a new policy or policy template

As a policy author you can define a new policy from scratch or from a template. See "Workflow for implementing policies" on page 293.

#### To add a new policy or a policy template

1 Click Add Policy at the Manage > Polices > Policy List screen.

See "Manage and add policies" on page 345.

2 Choose the type of policy you want to add at the **New Policy** screen.

Select Add a blank policy to add a new empty policy.

See "Policy components" on page 285.

Select **Add a policy from a template** to add a policy from a template.

See "Policy templates" on page 286.

Click **Next** to configure the policy or the policy template.

See "Configuring policies" on page 326.

See "Creating a policy from a template" on page 312.

Click Cancel to not add a policy and return to the Policy List screen.

## **Configuring policies**

The Manage > Policies > Policy List > Configure Policy screen is the home page for configuring policies.

Table 16-1 describes the workflow for configuring policies.

**Table 16-1** Configuring policies

Action	Description
Define a new policy, or edit an existing policy.	Add a new blank policy.
	See "Adding a new policy or policy template" on page 325.
	Create a policy from a template.
	See "Creating a policy from a template" on page 312.
	Select an existing policy at the <b>Manage &gt; Policies &gt; Policy List</b> screen to edit it.
	See "Manage and add policies" on page 345.
Enter a policy Name and Description.	The policy name must be unique in the policy group you deploy the policy to.
	See "Input character limits for policy configuration" on page 344.
	<b>Note:</b> The <b>Policy Label</b> field is reserved for the Symantec Data Insight Self-Service Portal.

**Table 16-1** Configuring policies (continued)

Action	Description
Select the <b>Policy Group</b> from the list where the policy is to be deployed.	The <b>Default Policy Group</b> is selected if there is no policy group configured.
	See "Creating and modifying policy groups" on page 348.
Set the <b>Status</b> for the policy.	You can enable (default setting) or disable a policy. A disabled policy is deployed but is not loaded into memory to detect incidents.
	See "Manage and add policies" on page 345.
	<b>Note:</b> The <b>Policy Actions</b> setting only applies to Classification policies. See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> .
Add a rule to the policy, or edit an existing rule.	Click Add Rule to add a rule.
	See "Adding a rule to a policy" on page 328.
	Select an existing rule to edit it.
Configure the rule with one or more conditions.	For a valid policy, you must configure at least one rule that declares at least one condition. Compound conditions and exceptions are optional.
	See "Configuring policy rules" on page 330.
Optionally, add one or more policy exceptions, or	Click Add Exception to add it.
edit an existing exception.	See "Adding an exception to a policy" on page 337.
	Select an existing exception to edit it.
Configure any exception(s).	See "Configuring policy exceptions" on page 340.
Save the policy configuration.	Click <b>Save</b> to save the policy configuration to the Enforce Server database.
	See "Policy components" on page 285.
Export the policy as a template.	Optionally, you can export the policy rules and exceptions as a template.
	See "Exporting policy detection as a template" on page 350.
Add one or more response rules to the policy.	You configure response rules independent of policies.
	See "Configuring response rules" on page 891.
	See "Adding an automated response rule to a policy" on page 350.

#### Adding a rule to a policy

At the Manage > Policies > Policy List > Configure Policy - Add Rule screen you add one or more rules to a policy.

You can add two types of rules to a policy: detection and group. If two or more rules in a policy are the same type, the system connects them by OR. If two or more rules in the same policy are different types, the system connects them by AND.

See "Policy detection execution" on page 308.

Note: Exceptions are added separate from rules. See "Adding an exception to a policy" on page 337.

#### To add one or more rules to a policy

Choose the type of rule (detection or group) to add to the policy.

To add a detection rule, select the **Detection** tab and click **Add Rule**.

To add a group (identity) rule, select the Groups tab and click Add Rule.

See "Policy matching conditions" on page 300.

2 Select the detection or the group rule you want to implement from the list of rules.

See Table 16-2 on page 328.

Select the prerequisite component, if required.

If the policy rule requires a Data Profile, Data Identifier, or User Group select it from the list.

Click **Next** to configure the policy rule.

See "Configuring policy rules" on page 330.

Adding policy rules **Table 16-2** 

Rule	Prerequisite	Description	
Content match conditions	Content match conditions		
Content Matches Regular Expression		See "Introducing regular expression matching" on page 598.	
Content Matches Exact Data	Exact Data Profile	See "About the Exact Data Profile and index" on page 371.  See "Choosing an Exact Data Profile" on page 322.	

Adding policy rules (continued) **Table 16-2** 

Rule	Prerequisite	Description
Content Matches Keyword		See "Introducing keyword matching" on page 584.
Content Matches Document Signature	Indexed Document Profile	See "Introducing Indexed Document Matching (IDM)" on page 462.
		See "Choosing an Indexed Document Profile" on page 323.
Content Matches Data Identifier	Data Identifier	See "Introducing data identifiers" on page 541.
		See "Selecting a data identifier breadth" on page 555.
Detect using Vector Machine Learning	VML Profile	See "Introducing Vector Machine Learning (VML)" on page 509.
		See "Configuring VML profiles and policy conditions" on page 513.
File Properties match conditions		
Message Attachment or File Type Match		See "About file type matching" on page 609.
Message Attachment or File Size Match		See "About file size matching" on page 611.
Message Attachment or File Name Match		See "About file name matching" on page 611.
Message/Email Properties and Attributes	Enterprise Vault integration	See "About implementing detection for Enterprise Vault Classification" on page 620.
		See the Enterprise Vault Data Classification Services Implementation Guide.
Custom File Type Signature	Rule enabled	See "About custom file type identification" on page 610.
	Custom script	See "Enabling the Custom File Type Signature condition in the policy console" on page 616.
Protocol and Endpoint match conditions		
Protocol Monitoring	Custom protocols (if any)	See "Introducing protocol monitoring for network" on page 626.
		See "Introducing protocol monitoring for mobile" on page 627.
Endpoint Monitoring		See "About endpoint protocol monitoring" on page 632.

**Table 16-2** Adding policy rules (continued)

Rule	Prerequisite	Description
Endpoint Device Class or ID	Custom device(s)	See "About endpoint device detection" on page 634.
Endpoint Location		See "About endpoint location detection" on page 634.
Groups (Identities) match condition	ons	
Sender/User Matches Pattern		See "Introducing described identity matching"
Recipient Matches Pattern		on page 643.
Sender/User based on a Directory Server Group	User Group	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.
Recipient based on a Directory Server Group		See "Configuring User Groups" on page 654.
Sender/User based on a Directory from:	Exact Data Profile	See "Introducing profiled Directory Group Matching (DGM)" on page 661.
Recipient based on a Directory from:		See "Configuring Exact Data profiles for DGM" on page 662.

## **Configuring policy rules**

At the Manage > Policies > Policy List > Configure Policy - Edit Rule screen, you configure a policy rule with one or more match conditions. The configuration of each rule condition depends on its type.

See Table 16-4 on page 331.

Configuring policy rules **Table 16-3** 

Step	Action	Description
Step 1	Add a rule to a policy, or modify a rule.	See "Adding a rule to a policy" on page 328.  To modify an existing rule, select the rule in the policy builder interface at the Configure Policy – Edit Rule screen.
Step 2	Name the rule, or modify a name.	In the <b>General</b> section of the rule, enter a name in the <b>Rule Name</b> field, or modify the name of an existing rule.

Configuring policy rules (continued) **Table 16-3** 

Step	Action	Description
Step 3	Set the rule severity.	In the <b>Severity</b> section of the rule, select or modify a "Default" severity level.
		In addition to the default severity, you can add multiple severity levels to a rule.
		See "Defining rule severity" on page 333.
Step 4	Configure the match condition.	In the <b>Conditions</b> section of the rule, you configure one or more match conditions for the rule. The configuration of a condition depends on its type.
		See Table 16-4 on page 331.
Step 5	Configure match counting (if	If the rule calls for it, configure how you want to count matches.
	required).	See "Configuring match counting" on page 334.
Step 6	Select components to match on (if available).	If the rule is content-based, select one or more available content rules to match on.
		See "Selecting components to match on" on page 336.
Step 7	Add and configure one or more additional match conditions	To define a compound rule, <b>Add</b> another match condition from the <b>Also Match</b> list.
	(optional).	Configure the additional condition according to its type (Step 4).
		See "Configuring compound match conditions" on page 342.
		<b>Note:</b> All conditions in a single rule must match to trigger an incident. See "Policy detection execution" on page 308.
Step 8	Save the policy configuration.	When you are done cofiguring the rule, click <b>OK</b> .
		This action returns you to the <b>Configure Policy</b> screen where you can <b>Save</b> the policy.
		See "Manage and add policies" on page 345.

Table 16-4 lists each of the available match conditions and provides links to topics for configuring each condition.

Configuring policy match conditions **Table 16-4** 

Rule	Description
Content match conditions	

Configuring policy match conditions (continued) **Table 16-4** 

Rule	Description		
Content Matches Regular Expression	See "Configuring the Content Matches Regular Expression condition" on page 600.		
Content Matches Exact Data from an Exact Data Profile	See "Configuring the Content Matches Exact Data policy condition" on page 396.		
Content Matches Keyword	See "Configuring the Content Matches Keyword condition" on page 591.		
Content Matches Document Signature	See "Configuring the Content Matches Document Signature policy condition" on page 497.		
Content Matches Data Identifier	See "Configuring the Content Matches data identifier condition" on page 552.		
Detect using Vector Machine Learning profile	See "Configuring the Detect using Vector Machine Learning Profile condition" on page 525.		
-	File Properties match conditions		
Message Attachment or File Type Match	See "Configuring the Message Attachment or File Type Match condition" on page 612.		
Message Attachment or File Size Match	See "Configuring the Message Attachment or File Size Match condition" on page 613.		
Message Attachment or File Name Match	See "Configuring the Message Attachment or File Name Match condition" on page 614.		
Message/Email Properties and Attributes	See "Configuring the Message/Email Properties and Attributes condition" on page 623.		
	See the Enterprise Vault Data Classification Services Implementation Guide.		
Custom File Type Signature	See "Configuring the Custom File Type Signature condition" on page 617.		
Protocol match conditions			
Network or Mobile Monitoring	See "Configuring the Protocol Monitoring condition for network detection" on page 628.		
	See "Configuring the Protocol Monitoring condition for mobile detection" on page 629.		
Endpoint Monitoring	See "Configuring the Endpoint Monitoring condition" on page 635.		
Endpoint Device Class or ID	See "Configuring the Endpoint Device Class or ID condition" on page 638.		
Endpoint Location	See "Configuring the Endpoint Location condition" on page 637.		

Tuble 10 4	Configuring policy materi conditions (continued)		
Rule	Description		
	Groups match conditions		
Sender/User Matches Pattern	See "Configuring the Sender/User Matches Pattern condition" on page 645.		
Recipient Matches Pattern	See "Configuring the Recipient Matches Pattern condition" on page 648.		
Sender/User based on a Directory Server Group	See "Configuring the Sender/User based on a Directory Server Group condition" on page 657.		
Sender/User based on a Directory from an Exact Data Profile	See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.		
Recipient based on a Directory Server Group	See "Configuring the Recipient based on a Directory Server Group condition" on page 658.		
Recipient based on a Directory from an Exact Data Profile	See "Configuring the Recipient based on a Profiled Directory condition" on page 664.		

Table 16-4 Configuring policy match conditions (continued)

#### **Defining rule severity**

The system assigns a severity level to a policy rule violation. The default setting is "High." You can configure the default, and add one or more additional severity levels.

See "Policy severity" on page 289.

Policy rule severity works with the Severity response rule condition. If you set the default policy rule severity level to "High" and define additional severity levels, the system does not assign the additional severity to the incident based on match count. The result is that if you have a response rule set to a match count severity level that is less than the default "High" severity, the response rule does not execute

See "Configuring the Severity response condition" on page 903.

#### To define policy rule severity

Configure a policy rule. 1

See "Configuring policy rules" on page 330.

2 Select a **Default** level from the **Severity** list.

The default severity level is the baseline level that the system reports. The system applies the default severity level to any rule match, unless additional severity levels override the default setting.

- 3 Click Add Severity to define additional severity levels for the rule.
  - If you add a severity level it is based on the match count.
- Select the desired severity level, choose the match count range, and enter the match count.
  - For example, you can set a Medium severity with X range to match after 100 matches have been counted.
- 5 If you add an additional severity level, you can select it to be the default severity.
- To remove a defined severity level, click the **X** icon beside the severity definition. 6

#### **Configuring match counting**

Some conditions let you specify how you want to count matches. Count all matches is the default behavior. You can configure the minimum number of matches required to cause an incident. Or, you can count all matches as one incident. If a condition supports match counting, you can configure this setting for both policy rules and exceptions.

See Table 16-6 on page 335.

**Table 16-5** Configuring match counting

Parameter	Condition type	Incident description
Check for existence	Simple	This configuration reports a match count of 1 if there are one or more matches; it does not count multiple matches. For example, 10 matches are one incident.
	Compound	This configuration reports a match count of 1 if there are one or more matches and ALL conditions in the rule or exception are set to check for existence.

Configuring match counting (continued) **Table 16-5** 

Parameter	Condition type	Incident description
Count all matches	Simple	This configuration reports a match count of the exact number of matches detected by the condition. For example, 10 matches count as 10 incidents.
	Compound	This configuration reports a match count of the sum of all condition matches in the rule or exception. The default is one incident per condition match and applies if any condition in the rule or exception is set to count all matches.
		For example, if a rule has two conditions and one is set to count all matches and detects four matches, and the other condition is set to check for existence and detects six matches, the reported match count is 10. If a third condition in the rule detects a match, the match count is 11.
	Only report incidents with	You can change the default one incident per match count by specifying the minimum number of matches required to report an incident.
at least _ matches	_	For example, in a rule with two conditions, if you configure one condition to count all matches and specify five as the minimum number of matches for each condition, a sum of 10 matches reported by the two conditions generates two incidents. You must be consistent and select this option for each condition in the rule or exception to achieve this behavior.
		<b>Note:</b> The count all matches setting applies to each message component you match on. For example, consider a policy where you specify a match count of 3 and configure a keyword rule that matches on all four message components (default setting for this condition). If a message is received with two instances of the keyword in the body and one instance of the keyword in the envelope, the system does not report this as a match. However, if three instances of the keyword appear in an attachment (or any other single message component), the system would report it as a match.
Count all unique matches	Only count unique matches	Unique match counting is new for Symantec Data Loss Prevention version 11.6 and is only available for Data Identifiers.  See "About unique match counting" on page 549.

**Table 16-6** Conditions that support match counting

Condition	Description
Content Matches Regular Expression	See "Introducing regular expression matching" on page 598.  See "Configuring the Content Matches Regular Expression condition" on page 600.
Content Matches Keyword	See "Introducing keyword matching" on page 584. See "Configuring the Content Matches Keyword condition" on page 591.

Condition Description Content Matches Document See "Configuring the Content Matches Document Signature policy condition" Signature (IDM) on page 497. Content Matches Data Identifier See "Introducing data identifiers" on page 541. See "Configuring the Content Matches data identifier condition" on page 552. See "Configuring unique match counting" on page 563. Recipient Matches Pattern See "Introducing described identity matching" on page 643. See "Configuring the Recipient Matches Pattern condition" on page 648.

**Table 16-6** Conditions that support match counting (continued)

## Selecting components to match on

The availability of one or more message components to match on depends on the type of rule or exception condition you implement.

See "Detection messages and message components" on page 305.

**Table 16-7** Match on components

Component	Description
Envelope	If the condition supports matching on the <b>Envelope</b> component, select it to match on the message metadata. The envelope contains the header, transport information, and the subject if the message is an SMTP email.
	If the condition does not support matching on the <b>Envelope</b> component, this option is grayed out.
	If the condition matches on the entire message, the <b>Envelope</b> is selected and cannot be deselected, and the other components cannot be selected.

**Table 16-7** Match on components (continued)

Component	Description
Subject	Certain detection conditions match on the <b>Subject</b> component for some types of messages.
	See "Detection messages and message components" on page 305.
	For the detection conditions that support subject component matching, you can match on the <b>Subject</b> for the following types of messages:
	<ul> <li>SMTP (email) messages from Network Monitor or Network Prevent for Email.</li> <li>NNTP messages from Network Monitor.</li> <li>Exchange email messages delivered by the Classification Server.</li> </ul>
	See the Enterprise Vault Data Classification Services Implementation Guide.
	To match on the <b>Subject</b> component, you must select (check) the <b>Subject</b> component and uncheck (deselect) the <b>Envelope</b> component for the policy rule. If you select both components, the system matches the subject twice because the message subject is included in the envelope as part of the header.
Body	If the condition matches on the <b>Body</b> message component, select it to match on the text or content of the message.
Attachment(s)	If the condition matches on the <b>Attachment(s)</b> message component, select it to detect content in files sent by, downloaded with, or attached to the message.

#### Adding an exception to a policy

At the Manage > Policies > Policy List > Configure Policy - Add Exception screen you add one or more exception conditions to a policy. Policy exceptions are executed before policy rules. If there is an exception match, the entire message is discarded.

See "Exception conditions" on page 307.

Note: You can create exceptions for all policy conditions, except the EDM condition Content Matches Exact Data From. In addition, Network Prevent for Web does not support synchronized DGM exceptions.

#### To add an exception to a policy

Add an exception to a policy.

To add a detection rule exception, select the **Detection** tab and click **Add** Exception.

To add a group rule exception, select the **Groups** tab and click **Add Exception**.

2 Select the policy exception to implement.

The Add Detection Exception screen lists all available detection exceptions that you can add to a policy.

The **Add Group Exception** screen lists all available group exceptions that you can add to a policy.

See Table 16-8 on page 338.

- 3 If necessary, choose the profile, data identifier, or user group.
- 4 Click **Next** to configure the exception.

See "Configuring policy exceptions" on page 340.

Selecting a policy exception **Table 16-8** 

Exception	Prerequisite	Description		
Content	Content			
Content Matches Regular Expression		See "Introducing regular expression matching" on page 598.		
Content Matches Keyword		See "Introducing keyword matching" on page 584.		
Content Matches Document Signature	Indexed Document Profile	See "Choosing an Indexed Document Profile" on page 323.		
Content Matches Data Identifier	Data Identifier	See "Introducing data identifiers" on page 541.		
		See "Selecting a data identifier breadth" on page 555.		
Detect using Vector Machine	VML Profile	See "Configuring VML policy exceptions" on page 526.		
Learning profile		See "Configuring VML profiles and policy conditions" on page 513.		
File Properties				
Message Attachment or File Type Match		See "About file type matching" on page 609.		

Selecting a policy exception (continued) **Table 16-8** 

Exception	Prerequisite	Description	
Message Attachment or File Size Match		See "About file size matching" on page 611.	
Message Attachment or File Name Match		See "About file name matching" on page 611.	
Message/Email Properties and Attributes	Enterprise Vault integration	See "About implementing detection for Enterprise Vault Classification" on page 620.	
		See the Enterprise Vault Data Classification Services Implementation Guide.	
Custom File Type Signature	Condition enabled Custom script added	See "About custom file type identification" on page 610.	
Protocol and Endpoint			
Network or Mobile Protocol		See "Introducing protocol monitoring for network" on page 626.	
		See "Introducing protocol monitoring for mobile" on page 627.	
Endpoint Protocol, Destination, Application		See "About endpoint protocol monitoring" on page 632.	
Endpoint Device Class or ID		See "About endpoint device detection" on page 634.	
Endpoint Location		See "About endpoint location detection" on page 634.	
Group (identity)			
Sender/User Matches Pattern		See "Introducing described identity matching" on page 643.	
Recipient Matches Pattern			
Sender/User based on a Directory Server Group	User Group	See "Introducing synchronized Directory Group Matching (DGM)" on page 653.	
Recipient based on a Directory		See "Configuring User Groups" on page 654.	
Server Group		<b>Note:</b> Network Prevent for Web does not support this type of exception. Use profiled DGM instead.	
Sender/User based on a Directory from:	Exact Data Profile	See "Introducing profiled Directory Group Matching (DGM)" on page 661.	
Recipient based on a Directory from:		See "Configuring Exact Data profiles for DGM" on page 662.	

## **Configuring policy exceptions**

At the Manage > Policies > Policy List > Configure Policy - Edit Exception screen you configure one or more conditions for a policy exception.

See Table 16-10 on page 341.

If an exception condition matches, the system discards the matched component from the system. This component is no longer available for evaluation.

See "Exception conditions" on page 307.

Configure policy exceptions **Table 16-9** 

Step	Action	Description
Step 1 Add a new policy exception, or	See "Adding an exception to a policy" on page 337.	
	edit an existing exception.	Select an existing policy exception to modify it.
Step 2	Name the exception, or edit an existing name or description.	In the <b>General</b> section, enter a unique name for the exception, or modify the name of an existing exception.
		Note: The exception name is limited to 60 characters.
Step 3	Select the components to apply the exception to (if available).	If the exception is content-based, you can match on the entire message or on individual message components.
		See "Detection messages and message components" on page 305.
		Select one of the Apply Exception to options:
		<ul> <li>Entire Message         This option applies the exception to the entire message.     </li> <li>Matched Components Only         This option applies the exception to each message component you select from the Match On options in the Conditions section of the exception.     </li> </ul>
Step 4	Configure the exception condition.	In the <b>Conditions</b> section of the <b>Configure Policy - Edit Exception</b> screen, define the condition for the policy exception. The configuration of a condition depends on the exception type.  See Table 16-10 on page 341.
Step 5	Add one or more additional conditions to the exception (optional).	You can add conditions until the exception is structured as desired.
		See "Configuring compound match conditions" on page 342.
		To add another condition to an exception, select the condition from the <b>Also Match</b> list.
		Click <b>Add</b> and configure the condition.

Configure policy exceptions (continued) **Table 16-9** 

Step	Action	Description
Step 6	Save and manage the policy.	Click <b>OK</b> to complete the exception definition process.
		Click <b>Save</b> to save the policy.
		See "Manage and add policies" on page 345.

Table 16-10 lists the exception conditions that you can configure, with links to configuration details.

Policy exception conditions available for configuration **Table 16-10** 

Exception	Description	
Content		
Content Matches Regular Expression	See "Configuring the Content Matches Regular Expression condition" on page 600.	
Content Matches Keyword	See "Configuring the Content Matches Keyword condition" on page 591.	
Content Matches Document Signature	See "Configuring the Content Matches Document Signature policy condition" on page 497.	
Content Matches Data Identifier	See "Configuring the Content Matches data identifier condition" on page 552.	
Detect using Vector Machine Learning Profile	See "Configuring VML policy exceptions" on page 526.	
File Properties		
Message Attachment or File Type Match	See "Configuring the Message Attachment or File Type Match condition" on page 612.	
Message Attachment or File Size Match	See "Configuring the Message Attachment or File Size Match condition" on page 613.	
Message Attachment or File Name Match	See "Configuring the Message Attachment or File Name Match condition" on page 614.	
Email/MAPI Attributes	See "Configuring the Message/Email Properties and Attributes condition" on page 623.	
	See the Enterprise Vault Data Classification Services Implementation Guide.	
Custom File Type Signature	See "Configuring the Custom File Type Signature condition" on page 617.	

Table 10-10 Toney exception conditions available for configuration (continue		
Exception	Description	
Network or Mobile Protocol	See "Configuring the Protocol Monitoring condition for network detection" on page 628.	
Endpoint Protocol or Destination	See "Configuring the Endpoint Monitoring condition" on page 635.	
Endpoint Device Class or ID	See "Configuring the Endpoint Device Class or ID condition" on page 638.	
Endpoint Location	See "Configuring the Endpoint Location condition" on page 637.	
Group (identity)		
Sender/User Matches Pattern	See "Configuring the Sender/User Matches Pattern condition" on page 645.	
Recipient Matches Pattern	See "Configuring the Recipient Matches Pattern condition" on page 648.	
Sender/User based on a Directory Server Group	See "Configuring the Sender/User based on a Directory Server Group condition" on page 657.	
Recipient based on a Directory Server Group	See "Configuring the Recipient based on a Directory Server Group condition" on page 658.	
Sender/User based on a Directory from an EDM Profile	See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.	
Recipient based on a Directory from and EDM Profile	See "Configuring the Recipient based on a Profiled Directory condition" on page 664.	

Table 16-10 Policy exception conditions available for configuration (continued)

## Configuring compound match conditions

You can create compound match conditions for policy rules and exceptions.

See "Configuring compound match conditions" on page 342.

The detection engine connects compound conditions with an AND. All conditions in the rule or exception must be met to trigger or except an incident.

See "Policy detection execution" on page 308.

You are not limited to the number of match conditions you can include in a rule or exception. However, the multiple conditions you declare in a single rule or exception should be logically associated. Do not mistake compound rules or exceptions with multiple rules or exceptions in a policy.

See "Use compound conditions to improve match accuracy" on page 363.

Table 16-11 Configure a compound policy rule or exception

Step	Action	Description
Step 1 Modify or configure an existing policy rule or exception.	You can add one or more additional match conditions to a policy rule at the Configure Policy – Edit Rule screen.	
	You can add one or more additional match conditions to a rule or exception at the <b>Configure Policy – Edit Rule</b> or <b>Configure Policy – Edit Exception</b> screen.	
Step 2	Select an additional match	Select the additional match condition from the <b>Also Match</b> list.
	condition.	This list appears at the bottom of the <b>Conditions</b> section for an existing rule or exception.
Step 3	Review the available conditions.	The system lists all available additional conditions you can add to a policy rule or exception.
		See "Adding a rule to a policy" on page 328.
		See "Adding an exception to a policy" on page 337.
Step 4	Add the additional	Click <b>Add</b> to add the additional match condition to the policy rule or exception.
condition.	Once added, you can collapse and expand each condition in a rule or exception.	
Step 5	Configure the additional	See "Configuring policy rules" on page 330.
	condition.	See "Configuring policy exceptions" on page 340.
Step 6	Select the same or any component to match.	If the condition supports component matching, specify where the data must match to generate or except an incident.
		Same Component – The matched data must exist in the same component as the other condition(s) that also support component matching to trigger a match.
		<b>Any Component</b> – The matched data can exist in any component that you have selected.
		See "About cross-component matching" on page 548.
Step 6	Repeat this process to	You can add as many conditions to a rule or exception as you need.
additional match condition to the rule or exception.		All conditions in a single rule or exception must match to trigger an incident, or to trigger the exception.
Step 7	Save the policy.	Click <b>OK</b> to close the rule or exception configuration screen.
		Click <b>Save</b> to save the policy configuration.

## Input character limits for policy configuration

When configuring a policy, consider the following input character limits for policy configuration components.

Input character limits for policy configuration Table 16-12

Configuration element	Input character limit
Name of a policy component, including:	60 characters
<ul> <li>Policy</li> <li>Rule</li> <li>Exception</li> <li>Group</li> <li>Condition</li> </ul>	<b>Note:</b> To import a policy as a template, the policy name must be less than 60 characters, otherwise it does not appear in the <b>Imported Templates</b> list.
Description of policy component.	255 characters
Name of Data Profile, including:  Exact Data Indexed Document Vector Machine Learning	255 characters
Data Identifier pattern limits	100 characters per line See "Using the data identifier pattern language" on page 573.

## Chapter

# Administering policies

This chapter includes the following topics:

- Manage and add policies
- Manage and add policy groups
- Creating and modifying policy groups
- Importing policy templates
- Exporting policy detection as a template
- Adding an automated response rule to a policy
- Removing policies and policy groups
- Viewing and printing policy details
- Downloading policy details
- Troubleshooting policies
- Updating EDM and IDM profiles to the latest version
- Updating policies after upgrading to the latest version

#### Manage and add policies

The **Manage > Policies > Policy List** screen is the home page for adding and managing policies. You implement policies to detect and report data loss.

See "Workflow for implementing policies" on page 293.

Table 17-1 lists and describes the actions you can take at the **Policy List** screen.

Policy List screen actions Table 17-1

Action	Description	
Add Policy	Click Add Policy to create a new policy.	
	See "Adding a new policy or policy template" on page 325.	
Modify Policy	Click anywhere in the policy row to modify an existing policy.	
	See "Configuring policies" on page 326.	
Activate Policy	Click the red circle icon by the policy name to activate the policy.	
Suspend Policy	Click the green circle icon by the policy name.	
	<b>Note:</b> By default, all solution pack policies are activated on installation of the solution pack.	
Sort Policies	Click any column header to sort the policy list.	
Remove Policy	Click the red X icon at the end of the policy row. On confirmation the system deletes the policy.	
	Note: You cannot remove a policy that has active incidents.	
	See "Removing policies and policy groups" on page 351.	
Export and Import Policy	See "Importing policy templates" on page 349.	
Templates	See "Exporting policy detection as a template" on page 350.	
Download Policy Details	Click <b>Download Policy Details</b> to download details for all policies in the <b>Policy List</b> . Symantec Data Loss Prevention exports the policy details as HTML files in a ZIP archive. Open the archive to view and print individual policy details.	
	See "Downloading policy details" on page 353.	
View and print policy details	To view policy details for a single policy, click the printer icon at the end of the policy row. To print the policy details, use the print feature of your web browser.	
	See "Viewing and printing policy details" on page 352.	

Table 17-2 lists and describes the display fields at the **Policy List** screen.

Policy List screen display fields **Table 17-2** 

Column	Description	
Name	View and sort by the name of the policy.	
	See "About Data Loss Prevention policies" on page 283.	

Column	Description	
Description	View the description of the policy.	
	See "Policy templates" on page 286.	
Policy Group	View and sort by the policy group to which the policy is deployed.	
	See "Policy groups" on page 287.	
Last Modified	View and sort by the date the policy was last updated.	
	See "Policy authoring privileges" on page 290.	
Misconfigured Policy	The policy icon is a yellow caution sign.	
	See "Policy components" on page 285.	
Active Policy	The policy icon is green. An active policy can detect incidents.	
Suspended Policy	The policy icon is red. A suspended policy is deployed but does not detect incidents.	

Table 17-2 Policy List screen display fields (continued)

## Manage and add policy groups

The **System > Servers > Policy Groups** screen lists the configured policy groups in the system.

From the Policy Groups screen you manage existing policy groups and add new ones.

Policy Groups screen actions **Table 17-3** 

Action	Description	
Add Policy Group	Click Add Policy Group to define a new policy group.	
	See "Policy groups" on page 287.	
Modify Policy Group	To modify an existing policy group, click the name of the group, or click the pencil icon to the far right of the row.	
	See "Creating and modifying policy groups" on page 348.	
Remove Policy Group  Click the red <b>X</b> icon to the far right of the row to delete that policy group from the A dialog box confirms the deletion.		
	<b>Note:</b> If you delete a policy group, you delete any policies that are assigned to that group.	
	See "Removing policies and policy groups" on page 351.	

Table 17-3 Policy Groups screen actions (continued)

Action	Description
View policies in a group	To view the policies deployed to an existing policy group, navigate to the <b>System &gt; Servers</b> > <b>Policy Groups &gt; Configure Policy Group</b> screen.
	See "Creating and modifying policy groups" on page 348.

**Table 17-4** Policy Groups screen display fields

Column	Description
Name	The name of the policy group.
Description	The description of the policy group.
Available Servers	The detection server to which the policy group is deployed.  See "Policy deployment" on page 288.
Last Modified	The date the policy group was last modified.

## Creating and modifying policy groups

At the System > Servers > Policy Groups screen you configure a new policy group or modify an existing one.

See "Policy groups" on page 287.

#### To configure a policy group

- Add a new policy group, or modify an existing one.
  - See "Manage and add policy groups" on page 347.
- 2 Enter the **Name** of the policy group, or modify an existing name.

Use an informative name. Policy authors and Enforce Server administrators rely on the policy group name when they associate the policy group with policies, roles, targets.

The name value is limited to 256 characters.

- 3 Enter a **Description** of the policy group, or modify an exiting description of an existing policy group.
- Select one or more **Servers** to assign the policy group to.

The system displays a check box for each detection server currently configured and registered with the Enforce Server.

- Select (check) the All Servers option to assign the policy group to all detection servers in your system. If you leave this checkbox unselected, you can assign the policy group to individual servers.
  - The All Discover Servers entry is not configurable because the system automatically assigns all policy groups to all Network Discover Servers. This feature lets you assign policy groups to individual Discover targets. See "Configuring the required fields for Network Discover targets" on page 1193.
- Deselect (uncheck) the **All Servers** option to assign the policy group to individual detection servers.
  - The system displays a check box for each server currently configured and registered with the Enforce Server.
  - Select each individual detection server to assign the policy group.
- 5 Click **Save** to save the policy group configuration.

Note: The Policies in this Group section of the Polices Group screen lists all the policies in the policy group. You cannot edit these entries. When you create a new policy group, this section is blank. After you deploy one or more policies to a policy group (during policy configuration), the **Policies in this Group** section displays each policy in the policy group.

See "Configuring policies" on page 326.

See "Policy deployment" on page 288.

#### Importing policy templates

You can import one or more policy templates to the Enforce Server. You must have policy system privileges to import policy templates.

See "Policy import and export" on page 292.

See "Exporting policy detection as a template" on page 350.

To import one or more policy templates to the Enforce Server

- Place one or more policy templates XML file(s) in the \SymantecDLP\Protect\config\templates directory on the Enforce Server host.
  - You can import multiple policies by placing them all in the templates directory.
- 2 Make sure that the directory and file(s) are readable by the "protect" system user.

- Log on to the Enforce Server Administration Console with policy authoring privileges.
- 4 Navigate to Manage > Policies > Policy List and click Add Policy.
- Choose the option Add a policy from a template and click Next.
- Scroll down to the bottom of the template list to the **Imported Templates** section.
  - You should see an entry for each XML file you placed in the templates directory.
- 7 Select the imported policy template and click Next to configure it. See "Configuring policies" on page 326.

#### Exporting policy detection as a template

You can export policy detection rules and exceptions in a template (XML file). You cannot export policy response rules. You can only export one policy template at a time.

See "Policy import and export" on page 292.

#### To export a policy as a template

- Log on to the Enforce Server administration console with administrator privileges.
- Navigate to the Manage > Policies > Policy List > Configure Policy screen for the policy you want to export.
- 3 At the bottom of the Configure Policy screen, click the Export this policy as a template link.
- Save the policy to a local or network destination of your choice.
  - For example, the system exports a policy named **Webmail** to the policy template file Webmail.xml which you can save to your local drive.

See "Importing policy templates" on page 349.

#### Adding an automated response rule to a policy

You can add one or more automated response rules to a policy to take action when that policy is violated.

See "About response rules" on page 875.

Note: Smart response rules are executed manually and are not deployed with policies.

#### To add an automated response rule to a policy

- Log on to the Enforce Server administration console with policy authoring privileges.
  - See "Policy authoring privileges" on page 290.
- Navigate to the Manage > Policies > Policy List > Configure Policy screen for the policy you want to add a response rule to.
- 3 Select the response rule you want to add from those available in the drop-down menu.
  - Policies and response rules are configured separately. To add a response rule to a policy, the response rule must first be defined and saved independently.
  - See "Implementing response rules" on page 886.
- 4 Click **Add Response Rule** to add the response rule to the policy.
- 5 Repeat the process to add additional response rules to the policy.
- 6 **Save** the policy when you are done adding response rules.
- Verify that the policy status is green after adding the response rule to the policy. See "Manage and add policies" on page 345.

Note: If the policy status is a yellow caution sign, the policy is misconfigured. The system does not support certain pairings of detection rules and automated response rule actions. See Table 70-2 on page 1366.

#### Removing policies and policy groups

Consider the following guidelines before you delete a policy or a policy group from the Enforce Server.

		1 70 1
Action	Description	Guideline
Remove a policy	If you attempt to delete a policy that has associated incidents, the system does not let you remove the policy.	If you want to delete a policy, you must first delete all incidents that are associated with that policy from the Enforce Server.
		See "Manage and add policies" on page 345.
		An alternative is to create an undeployed policy group (one that is not assigned to any detection servers). This method is useful to maintain legacy policies and incidents for review without keeping these policies in a deployed policy group.  See "Policy import and export" on page 292.
Remove a policy group	If you attempt to delete a policy group that contains one or more policies, the system displays an error message. And, the policy group is not deleted.	Before you delete a policy group, remove any policies from that group by either deleting them or assigning them to different policy groups.  See "Manage and add policy groups" on page 347.
		If you want to remove a policy group, create a maintenance

**Table 17-5** Guidelines for removing policies and policy groups

See "About Data Loss Prevention policies" on page 283.

See "Policy groups" on page 287.

## Viewing and printing policy details

You can view and print policy details from the **Policy List** screen.

You must have the Author Policies privilege for the policies you want to view and print.

the maintenance group.

policy group and move the policies you want to remove to

See "Creating and modifying policy groups" on page 348.

See "Policy authoring privileges" on page 290.

See "Viewing, printing, and downloading policy details" on page 295.

#### To view and print policy details

- Navigate to Manage > Policies > Policy List and click the printer icon at the end of the policy row.
  - The **Policy Snapshot** screen appears.
- 2 View the general policy information, detection rules, and response rules on the Policy Snapshot screen.
- 3 To print the policy details, use the **Print** command in your web browser from the Policy Snapshot screen.

#### Downloading policy details

You can download a ZIP archive of details for all policies in the **Policy List**. The ZIP archive contains HTML documents with details for each policy on the Policy List, as well as an index file to make it easier to find the policy details you want. The files are titled using the policy ID, such as 123.html. The index file is titled downloaded policies DATE.html, and it contains the policy name, description, status, policy group, and last modified date of all policies in the download, as well as links to the policy details.

You must have the Author Policies privilege for the policies you want to download.

See "Policy authoring privileges" on page 290.

See "Viewing, printing, and downloading policy details" on page 295.

#### To download policy details

- Navigate to Manage > Policies > Policy List and click Download Policy Details.
- In the Open File dialog box, click select Save File, then click OK.
- To view details for a policy, extract the files from the ZIP archive, then open the file you want to view. Use the index file to search through the downloaded policies by policy name, description, status, policy group, or last modified date.
  - The **Policy Snapshot** screen appears.
- To print the policy details, use the **Print** command in your web browser from the Policy Snapshot screen.

#### Troubleshooting policies

Table 17-6 lists log files to consult for troubleshooting policies.

Log file	Description	
VontuMonitor.log	Logs when policies and profiles are sent from the Enforce Server to detection servers and endpoint servers. Displays JRE errors.	
	See "Debug log files" on page 247.	
detection_operational.log	Log the loading of policies and detection execution.	
detection_operational_trace.log	See "Operational log files" on page 244.	
FileReader.log	Logs when an index file is loaded into memory. For EDM, look for the line "loaded database profile." For IDM look for the line: "loaded document profile."	
	See "Debug log files" on page 247.	
Indexer.log	Logs the operations of the Indexer process to generate EDM and IDM indexes.	
	See "Debug log files" on page 247.	

**Table 17-6** Log files for troubleshooting policies

See "About log files" on page 243.

See "Log collection and configuration screen" on page 252.

See "Configuring server logging behavior" on page 252.

See "Collecting server logs and configuration files" on page 257.

See "Log files for troubleshooting VML training and policy detection" on page 531.

See "Advanced server settings" on page 203.

See "Advanced agent settings" on page 1414.

#### Updating EDM and IDM profiles to the latest version

Symantec Data Loss Prevention version 12.5 provides several significant updates to Exact Data Matching (EDM) and Indexed Document Matching (IDM) technologies. See the Symantec Data Loss Prevention What's New and What's Changed Guide for more information.

To use these new features on an upgraded system, you must reindex your data and document sources. Before deploying an index into production, you should test the updated profile and policies based on it to ensure that they detect data loss as expected on the upgraded system.

Table 17-7 lists the reindexing requirements for updating your EDM and IDM profiles to version 12.5 and provides links for more information.

Table 17-7	Raindaving	raquiramants	for FDM	MGI bac	data	nrnfilac

Technology and features	Required action(s)	More information
Exact Data Matching (EDM)  Multi-token matching Proportional proximity range	If you have existing Exact Data profiles supporting EDM policies and you want to use new EDM features, before upgrading the detection server(s) you must:  Reindex each structured data source using a 12.5-compatible EDM indexer, and Load each index into a 12.5-generated Exact Data profile.	See "Updating EDM indexes to version 12.5" on page 416. In addition, refer to the chapter "Updating EDM indexes to version 12.5" in the Symantec Data Loss Prevention Administration Guide and the online Help.
Indexed Document Matching (IDM)  Exact match IDM on the endpoint (Agent IDM)	If you have existing Indexed Document profiles supporting IDM policies and you want to use Agent IDM, after upgrading to 12.5 you must:  Disable two-tier detection on the Endpoint Server, and Reindex each document data source so that the endpoint index is generated and deployed to the Endpoint Server for download by the DLP Agent.	See "Using agent IDM after upgrade to version 12.5" on page 494.  Or, refer to the topic "Using Agent IDM after upgrade to version 12.5" in the Symantec Data Loss Prevention Administration Guide and the online Help.

#### Updating policies after upgrading to the latest version

Symantec Data Loss Prevention provides several updates to policy templates. On upgrade the system updates the system-defined policy templates. Policies you have created based on an upgraded policy template are not changed so that configurations you have made are not overwritten. If you have created policies based on one or more of the updated policy templates, you should update your policies so that they are current.

The HIPAA and HITECH (including PHI) and the Caldicott Report policy templates are updated with recent Drug, Disease, and Treatment keyword list terminology based on information from the U.S. Federal Drug Administration (FDA) and other sources. Symantec recommends that you update policies derived from these templates with the updated Drug, Disease, and Treatment keyword lists.

See "Updating the Drug, Disease, and Treatment keyword lists for your HIPAA and Caldicott policies" on page 594.

In addition, policy templates that use data identifier patterns to detect Social Security Numbers (SSNs) are updated to use the Randomized US SSN data identifier, which detects both traditional and randomized SSNs. Symantec recommends that you update your SSN policies to use the Randomized US SSN data identifier.

See "Updating policies to use the Randomized US SSN data identifier" on page 569.

Table 17-8 lists the policy templates updated for this release of Symantec Data Loss Prevention.

**Table 17-8** Policy templates updated in Data Loss Prevention version 12.5

Updated template	Updated component(s)	Policy description
Caldicott Report	Drug, Disease, and Treatment keyword lists	See "Caldicott Report policy template" on page 802.
Customer Data Protection	Randomized US SSN data identifier	See "Customer Data Protection policy template" on page 808.
Employee Data Protection	Randomized US SSN data identifier	See "Employee Data Protection policy template" on page 815.
FACTA 2003 (Red Flag Rules)	Randomized US SSN data identifier	See "FACTA 2003 (Red Flag Rules) policy template" on page 818.
Gramm-Leach-Bliley	Randomized US SSN data identifier	See "Gramm-Leach-Bliley policy template" on page 824.
HIPAA and HITECH (including PHI)	Drug, Disease, and Treatment keyword lists Randomized US SSN data identifier	See "HIPAA and HITECH (including PHI) policy template" on page 826.
State Data Privacy	Randomized US SSN data identifier	See "State Data Privacy policy template" on page 859.
US Social Security Numbers	Randomized US SSN data identifier	See "US Social Security Numbers policy template" on page 867.

# Best practices for authoring policies

This chapter includes the following topics:

- Best practices for authoring policies
- Develop a policy strategy that supports your data security objectives
- Use a limited number of policies to get started
- Use policy templates but modify them to meet your requirements
- Use the appropriate match condition for your data loss prevention objectives
- Test and tune policies to improve match accuracy
- Start with high match thresholds to reduce false positives
- Use a limited number of exceptions to narrow detection scope
- Use compound conditions to improve match accuracy
- Author policies to limit the potential effect of two-tier detection
- Use policy groups to manage policy lifecycle
- Follow detection-specific best practices

#### Best practices for authoring policies

This section provides general policy authoring best practices for Symantec Data Loss Prevention. This section assumes that the reader has general familiarity with policy authoring, including the configuration, testing, and deployment of policies, detection rules, match conditions, and policy exceptions

See "About Data Loss Prevention policies" on page 283.

See "Detecting data loss" on page 296.

Best practices are not intended to provide detailed troubleshooting guidance. Rather, it is goal of this section to provide best practices that, when followed, will proactively help to reduce the need for policy troubleshooting and support.

Table 18-1 Summary of policy authoring best practices

Best practice	Description
Develop a policy strategy that supports your data security objectives.	See "Develop a policy strategy that supports your data security objectives" on page 359.
Use a limited number of policies to get started.	See "Use a limited number of policies to get started" on page 359.
Use policy templates but modify them to meet your requirements.	See "Use policy templates but modify them to meet your requirements" on page 360.
Use policy groups to manage policy lifecycle.	See "Use policy groups to manage policy lifecycle" on page 365.
Use the appropriate match condition for your data loss prevention objectives.	See "Use the appropriate match condition for your data loss prevention objectives" on page 360.
Test and tune policies to improve match accuracy.	See "Test and tune policies to improve match accuracy" on page 361.
Start with high match thresholds to reduce false positives.	See "Start with high match thresholds to reduce false positives" on page 362.
Use a limited number of exceptions to narrow detection scope.	See "Use a limited number of exceptions to narrow detection scope" on page 363.
Use compound conditions to improve match accuracy.	See "Use compound conditions to improve match accuracy" on page 363.
Author policies to limit the potential effect of two-tier detection.	See "Author policies to limit the potential effect of two-tier detection" on page 364.
Follow detection-specific best practices.	See "Follow detection-specific best practices" on page 365.

#### Develop a policy strategy that supports your data security objectives

The goal of detection is to achieve accurate results based on true policy matches. Well-authored policies should accurately detect the data you want to protect with minimal false positives. Through the use of well-defined policies that implement the right type and combination of rules, conditions, and exceptions, you can achieve accurate detection results and prevent the loss of the most critical data in your enterprise

There are two general approaches to developing a data loss prevention policy strategy:

- Information-driven Identify sensitive data and author policies to prevent it from being lost.
- Regulation-driven

   Review government and industry regulations and author policies to comply with them.

Table 18-2 describes these two approaches in more detail.

**Table 18-2** Policy detection approaches

Approach	Description
Information-driven	With this approach you start by identifying specific data items and data combinations you want to protect. Examples of such data may include fields profiled from a database, a list of keywords, a set of users, or a combination of these elements. You then group similar data items together and create policies to identify and protect them. This approach works best when you have limited access to the data or no particular concerns about a given regulation.
Regulation-driven	With this approach you begin with a policy template based on the regulations with which you must comply. Examples of such templates may include HIPAA or FACTA. Also, begin with a large set of data (such as customer or employee data). Use the high-level requirements stipulated by the regulations as the basis for this approach. Then, decide what sensitive data items and documents in your enterprise meet these requirements. These data items become the conditions for the detection rules and exceptions in your policies.

#### Use a limited number of policies to get started

The policy detection rules you implement are based on your organization's information security objectives. The actions you take in response to policy violations are based on your organization's compliance requirements. In general you should start small with policy detection. Enable one or two policy templates, or a few simple conditions, such as keyword matching. Review the incidents each policy detects. Tune the results before you implement response rules to take action.

Generally it is better to have fewer policies that are configured to address specific data loss prevention objectives rather than many policies that attempt to address all of your security requirements. Having too many policies can impact the performance of the system and can lead to too many false positives.

See "Test and tune policies to improve match accuracy" on page 361.

#### Use policy templates but modify them to meet your requirements

Policy templates provide an excellent starting point for authoring policies. Symantec Data Loss Prevention provides 65 pre-built policy templates that contain detection rules and conditions for many different types of use cases, including regulatory compliance, data protection, security enforcement, and acceptable use scenarios.

You should use the system-provided policy templates as starting points for your policies. Doing so will save time and help you avoid errors and information gaps in your policies since the detection methods are predefined. However, for most situations you will want to modify the policy template and tailor it for your specific environment. Deploying a policy template out-of-the-box without configuring it for your environment is not recommended.

See "Creating a policy from a template" on page 312.

#### Use the appropriate match condition for your data loss prevention objectives

To prevent data loss, it is necessary to accurately detect all types of confidential data wherever that data is stored, copied, or transmitted. To meet your data security objectives, you need to implement the appropriate detection methods for the type of data you want to protect. The recommendation is to determine the detection methods that work best for you, and tune the policies as necessary based on the results of your detection testing.

Table 18-3 describes the primary use case for each type of policy match condition provided by Data Loss Prevention.

**Table 18-3** Match conditions compared

Type of data you want to protect	Condition	Matching
Personally Identifiable Information (PII), such as SSNs, CCNs, and Driver's License numbers	EDM	Exact profiled data
	Data Identifiers	Described, validated data patterns

Type of data you want to protect	Condition	Matching
Confidential documents, such as Microsoft Word,	IDM	Exact file contents
PowerPoint, PDF, etc.		Partial file contents (derivative)
	VML	Similar file contents
Confidential files and images, such as CAD	IDM	Exact file
drawings	File Properties	File context (type, name, size)
Words and phrases, such as "Confidential" or "Proprietary"	Keywords	Exact words, phrases, proximity
Characters, strings, text	Regular Expressions	Described text
Network and endpoint communications	Protocol and Endpoint	Protocols, destinations, monitoring
Determined by the identity of the user, sender,	Synchronized DGM	Exact identity from LDAP server
recipient	Profiled DGM	Exact profiled identity
	Sender/user, recipient	Described identity patterns
Describes a document, such as author, title, date, etc.	Content-based conditions	File type metadata

Match conditions compared (continued) **Table 18-3** 

### Test and tune policies to improve match accuracy

When you create detection policies, there are two common detection problems to avoid. If you create a policy that is too general or too broad, it generates incidents when no real match has occurred (false positive). On the other hand, if a policy has rules that are too specific or narrow about the data it detects, the policy may miss some of the matches you intend to catch (false negatives). Table 18-4 describes these common problems in more detail.

To reduce false positives and negatives, you need to tune your policies. The best way to tune detection is to identify a single, specific use case that is a priority, such as protecting source code for a particular product. You then create a single policy—either from scratch or based on a template, depending on your DLP strategy—containing one or two detection rules and test the policy to see how many (quantity) and the types (quality) of incidents the policy generates. Based on these initial results, you adjust the detection rule(s) as needed. If the policy generates more false positives than you want, make the detection rule(s) more specific by fine-tuning the existing match conditions, adding additional match conditions, and

creating policy exceptions. If the policy does not detect some incidents, make the detection condition(s) less specific.

As your policies mature, it is important to continuously test and tune them to ensure ongoing accuracy.

See "Follow detection-specific best practices" on page 365.

**Table 18-4** Common detection problems to avoid

Problem	Cause	Description
False positives	Policy rules too general or broad	False positives create high costs in time and resources that are required to investigate and resolve apparent incidents that are not actual incidents. Since many organizations do not have the capacity to manage excess false positives, it is important that your policies define contextual rules to improve accuracy.
		For example, a policy is designed to protect customer names and generates an incident for anything that contains a first and last name. Since most messages contain a name—in many cases both first and last names—this policy is too broad and general. Although it may catch all instances of customer names being sent outside the network, this policy will return too many false positives by detecting email messages that do not divulge protected information. First and last names require a much greater understanding of context to determine if the data is confidential
False negatives	Policy rules too tight or narrow	False negatives obscure gaps in security by allowing data loss, the potential for financial losses, legal exposure, and damage to the reputation of an organization. False negatives are especially dangerous because you do not know you have lost sensitive data.
		For example, a policy that contains a keyword match on the word "confidential" but also contains a condition that excludes all Microsoft Word documents would be too narrow and be suspect to false negatives because it would likely miss detecting many actual incidents contained in such documents

See "Start with high match thresholds to reduce false positives" on page 362. See "Use a limited number of exceptions to narrow detection scope" on page 363.

See "Use compound conditions to improve match accuracy" on page 363.

## Start with high match thresholds to reduce false positives

For content-based detection rules, there is a configuration setting that lets you "count all matches" but only report an incident after a threshold number of matches has been reached. The general recommendation is to start with high match

thresholds for your content-based detection policies. As you tune your policies you can reduce the match thresholds to be more precise.

See "Configuring match counting" on page 334.

## Use a limited number of exceptions to narrow detection scope

You can implement exception conditions for any detection rule, except EDM rules. The limited use of exception conditions can help to reduce false positives by narrowing the scope of policy detection. However, if you need to use several exceptions in a single policy to achieve the desired detection results, reconsider the design of the policy. Make sure the policy is well-defined and uses the proper match conditions.

Caution: Too many compound exceptions in a policy can cause system performance issues. You should avoid the use of compound exceptions as much as possible.

It is important to understand how exception conditions work so you can use them properly. Exception conditions disqualify messages from creating incidents. Exception conditions are checked first by the detection server before match conditions. If the exception condition matches, the system immediately discards the entire message or message component that met the exception. There is no support for match-level exceptions. Once the message or message component is discarded by meeting an exception, the data is no longer available for policy evaluation.

See "Exception conditions" on page 307.

See "Use compound conditions to improve match accuracy" on page 363.

## Use compound conditions to improve match accuracy

Compound conditions can help you improve the match accuracy of your policies. Suppose you are concerned about Microsoft Word documents leaving the network. Initially, you add a policy that uses an attachment type condition to catch all Word files. You quickly discover that too many messages contain Word file attachments that do not divulge protected information. When you examine the incidents more closely, you realize that you are more concerned with Word files that contain the word CONFIDENTIAL. In this case you can convert the attachment type condition to a compound rule by adding a keyword rule for the word CONFIDENTIAL. Such a configuration would achieve more accurate detection results.

See "Compound conditions" on page 308.

## Author policies to limit the potential effect of two-tier detection

The Exact Data Matching (EDM) and profiled Directory Group Matching (DGM) conditions require two-tier detection. For these conditions, the DLP Agent must send the data to the Endpoint Server for evaluation. Indexed Document Matching (IDM) uses two-tier detection if it is enabled.

See "Two-tier detection for DLP Agents" on page 309.

On the endpoint the DLP Agent executes the least expensive rules first. If you are deploying a policy to the endpoint that requires two-tier detection, you can author the policy in such a way to limit the potential effect of two-tier detection.

Table 18-5 provides some considerations for authoring policies to limit the potential effect of two-tier detection.

See "Detection messages and message components" on page 305.

**Table 18-5** Policy configurations for two-tier detection rules

Two-tier match condition	Policy configuration
Exact Data Matching (EDM)	For EDM policies, consider including Data Identifier rules OR'd with EDM rules. For example, for a policy that uses an EDM condition to match social security numbers, you could add a second rule that uses the SSN Data Identifier condition. The Data Identifier does not require two-tier detection and is evaluated locally by the DLP Agent. If the DLP Agent is not connected to the Endpoint Server when the DLP Agent receives the data, the DLP Agent can still perform SSN pattern matching based on the Data Identifier condition.
	See "Combine Data Identifiers with EDM rules to limit the impact of two-tier detection" on page 460.
	For example policy configurations, each of the policy templates that provide EDM conditions also provide corresponding Data Identifier conditions.
	See "Choosing an Exact Data Profile" on page 322.

Two-tier match condition	Policy configuration	
Indexed Document Matching (IDM)	For IDM policies that match file contents, consider using VML rules OR'd with IDM rules. VML rules do not require two-tier detection and are executed locally by the DLP Agent. If you do not need to match file contents exactly, you may want to use VML instead of IDM.	
	See "Use the appropriate match condition for your data loss prevention objectives" on page 360.	
	If you are only concerned with file matching, not file contents, consider using compound file property rules instead of IDM. File property rules do not require two-tier detection.	
	See "Use compound file property rules to protect design and multimedia files" on page 618.	
Directory Group Matching (DGM)	For the synchronized DGM Recipient condition, consider including a Recipient Matches Pattern condition OR'd with the DGM condition. The pattern condition does not require two-tier detection and is evaluated locally by the DLP Agent.	
	See "About two-tier detection for synchronized DGM" on page 654.	

Policy configurations for two-tier detection rules (continued) **Table 18-5** 

## Use policy groups to manage policy lifecycle

Use policy groups to test policies before using them in production. Create a test policy group to which only you have access. Then, create policies and add them to the test policy group. Review the incidents your test policies capture. After you tune the policies and confirm that they capture the expected incidents, you can rename the policy group and grant the appropriate roles access to it. You can also use policy groups to manage legacy policies, as well as policies you want to import or export.

See "Policy groups" on page 287.

See "Removing policies and policy groups" on page 351.

## Follow detection-specific best practices

In additional to these general policy authoring considerations, you should be aware of and keep in mind policy tuning considerations specific to each type of match condition.

Table 18-6 lists detection specific considerations, with links to topics for more information.

Best practices for specific detection methods **Table 18-6** 

<b>Detection method</b>	Description	
EDM	See "Best practices for using EDM" on page 451.	
IDM	See "Best practices for using IDM" on page 499.	
VML	See "Best practices for using VML" on page 532.	
Data identifiers	See "Best practices for using data identifiers" on page 579.	
Keywords	See "Best practices for using keyword matching" on page 595.	
Regular expressions	See "Best practices for using regular expression matching" on page 601.	
Non-English language detection	See "Best practices for detecting non-English language content" on page 605.	
File properties	See "Best practices for using file property matching" on page 618.	
Network protocols	See "Best practices for using network protocol matching" on page 630.	
Endpoint events	See "Best practices for using endpoint detection" on page 642.	
Described identities	See "Best practices for using described identity matching" on page 650.	
Synchronized DGM	See "Best practices for using synchronized DGM" on page 659.	
Profiled DGM	See "Best practices for using profiled DGM" on page 665.	
Metadata detection	See "Best practices for using metadata detection" on page 694.	

# Detecting content using Exact Data Matching (EDM)

This chapter includes the following topics:

- Introducing Exact Data Matching (EDM)
- Configuring Exact Data profiles
- Configuring EDM policies
- Using multi-token matching
- Updating EDM indexes to version 12.5
- Memory requirements for EDM
- Remote EDM indexing
- Best practices for using EDM

## **Introducing Exact Data Matching (EDM)**

Exact Data Matching (EDM) is designed to protect your most sensitive content. You can use EDM to detect personally identifiable information (PII)—such as social security numbers, bank account numbers, credit card numbers—confidential customer and employee records, and other confidential data stored in a structured data source, such as a database, directory server, or a structured data file such as CSV or spreadsheet.

To implement EDM policies, you identify and prepare the data you want to protect. You create an **Exact Data Profile** and index the structured data source using the Enforce Server administration console, or remotely using the Remote EDM Indexer. During the indexing process, the system fingerprints the data by accessing and

extracting the text-based content, normalizing it, and securing it using a nonreversible hash. You can schedule indexing on a regular basis so the data is current.

Once you have profiled the data, you configure the Content Matches Exact Data condition to match individual pieces of the indexed data. For increased accuracy you can configure the condition to match combinations of data fields from a particular record. The EDM policy condition matches on data coming from the same row or record of data. For example, you can configure the EDM policy condition to look for any three of First Name, Last Name, SSN, Account Number, or Phone Number occurring together in a message and corresponding to a record from your customer database.

Once the policy is deployed to one or more detection servers, the system can detect the data you have profiled in either structured or unstructured format. For example, you could deploy the EDM policy to a Network Discover Server and scan data repositories for confidential data matching data records in the index. Or, you could deploy the EDM policy to a Network Prevent for Email Server to detect records in email communications and attachments, such as Microsoft Word files. If the attachment is a spreadsheet, such as Microsoft Excel, the EDM policy can detect the presence of confidential records there as well.

See "About the Exact Data Profile and index" on page 371.

#### About using EDM to protect content

To understand how EDM works, consider the following example. Your company maintains an employee database that contains the following column fields:

- First Name
- Last Name
- SSN
- Date of Hire
- Salary

In a structured data format such as a database, each row represents one record, with each record containing values for each column data field. In this example, each row in the database contains information for one employee, and you can use EDM to protect each record. For example, one row in the data source file contains the following pipe ("|") delimited record:

First Name | Last Name | SSN | Date of hire | Salary

```
Bob | Smith | 123-45-6789 | 05/26/99 | $42500
```

You create an Exact Data Profile and index the data source file. When you configure the profile, you map the data field columns to system-defined patterns and validate the data. You then configure the EDM policy condition that references the Exact Data Profile. In this example, the condition matches if a message contains all five data fields.

The detection server reports a match if it detects the following in any inbound message:

Bob Smith 123-45-6789 05/26/99 \$42500

But, a message containing the following does not match because that record is not in the index:

Betty Smith 000-00-0000 05/26/99 \$42500

If you limited the condition to matching only the Last Name, SSN, and Salary column fields, the following message is a match because it meets the criteria:

Robert, Smith, 123-45-6789, 05/29/99, \$42500

Finally, the following message contents do not match because the value for the SSN is not present in the profile:

Bob, Smith, 415-789-0000, 05/26/99, \$42500

See "Configuring Exact Data profiles" on page 378.

#### EDM policy features

EDM policy matching involves searching for indexed content in a given message and generating an incident if a match is found within the defined proximity range.

Policy matching features of EDM include the following:

- You can select any number of columns to be matched from a given data source.
- You can define exclude combinations so that matches against those combinations are not reported.
- When creating the index, the system provides pattern validation for social security numbers, credit card numbers, U.S. and Canada phone numbers and ZIP codes, email and IP addresses, numbers and percents.
- There is an editable stop word dictionary you can use to prevent single token stopwords from matching.
- The system provides match highlighting at the incident snapshot screen.
- You can use a where clause in the EDM rule and matches that do not satisfy the where clause are ignored.
- You can use Data Owner Exception to ignore detection based on the sender or recipient's email address or domain.

- You can use profiled Directory Group Matching (DGM) to match on senders or recipients of data based on email address, IM handle, or Windows user name.
- Proximity matching range that is proportional to the number of required matches set in the policy condition.
- Full support for single- and multi-token cell indexing and matching. A multi-token is a cell that his indexed that contains two or more words.

See "EDM policy templates" on page 370.

See "EDM policy templates" on page 370.

See "EDM policy templates" on page 370.

#### EDM policy templates

Symantec Data Loss Prevention provides several policy templates that feature EDM. If you use one of these templates, the system lets you validate your Exact Data Profile against the template when you are configuring the profile.

- Caldicott Report See "Caldicott Report policy template" on page 802.
- Customer Data Protection See "Customer Data Protection policy template" on page 808.
- Data Protection Act 1988 See "Data Protection Act 1998 (UK) policy template" on page 810.
- Employee Data Protection See "Employee Data Protection policy template" on page 815.
- FU Data Protection Directives See "Data Protection Directives (EU) policy template" on page 811.
- Export Administration Regulations (EAR) See "Export Administration Regulations (EAR) policy template" on page 817.
- FACTA 2003 (Red Flag Rules) See "FACTA 2003 (Red Flag Rules) policy template" on page 818.
- Gramm-Leach-Bliley See "Gramm-Leach-Bliley policy template" on page 824.
- HIPAA and HITECH (including PHI) See "HIPAA and HITECH (including PHI) policy template" on page 826.
- Human Rights Act 1998 See "Human Rights Act 1998 policy template" on page 830.
- International Traffic in Arms Regulations (ITAR)

See "International Traffic in Arms Regulations (ITAR) policy template" on page 832.

- Payment Card Industry Data Security Standard See "Payment Card Industry (PCI) Data Security Standard policy template" on page 845.
- PIPFDA See "PIPEDA policy template" on page 846.
- Price Information See "Price Information policy template" on page 848.
- Resumes See "Resumes policy template" on page 852.
- State Data Privacy See "SEC Fair Disclosure Regulation policy template" on page 855.

See "Creating and modifying Exact Data Profiles" on page 385.

See "Leverage EDM policy templates when possible" on page 456.

#### About the Exact Data Profile and index

The **Exact Data Profile** is the user-defined configuration you create to index the data source and map the data. The index is a secure file (or set of files) that contains hashes of the exact data values from each field in your data source, along with information about those data values. The index does not contain the data values themselves.

The index that is generated consists of one or more binary DataSource.rdx files, each with space to fit into random access memory (RAM) on the detection server(s). For a large data source file, the system may break the data into several \*.rdx files. By default, Symantec Data Loss Prevention stores index files in \SymantecDLP\Protect\index (on Windows) or in /var/SymantecDLP/index (on Linux) on the Enforce Server.

Symantec Data Loss Prevention automatically deploys EDM indexes (\*.rdx files) to the index directory on all detection servers. When an active policy that references an EDM profile is deployed to a detection server, the detection server loads the corresponding EDM index into RAM. If a new detection server is added after an index has been created, the \*.rdx files in the index folder on the Enforce Server are deployed to the index folder on the new detection server. You cannot manually deploy index files to detection servers.

At run-time during detection, the system converts input content into hashed data values using the same algorithm it employs for indexes. It then compares data

values from input content to those in the appropriate index file(s), identifying matches.

See "Creating and modifying Exact Data Profiles" on page 385.

See "Memory requirements for EDM" on page 421.

#### About the exact data source file

The data source file is a flat file containing data in a standard delimited format (pipe or tab) that has been extracted from a database, spreadsheet, or other structured data source, and cleansed for profiling. You upload the data source file to the Enforce Server when you are defining the **Exact Data Profile**. For example, by exporting data from a database (performing a "data dump"), the resulting \*.dat file can be used as the data source for your EDM profile.

See "Creating the exact data source file for EDM" on page 379.

You can use the SQL pre-indexer to index the data source directly. However, this approach has limitations because in most cases the data must first be cleansed before it is indexed.

See "Remote EDM indexing" on page 432.

The data source file must contain at least one unique column field. Some examples of unique column fields include social security number, drivers license number, and credit card number.

See "Best practices for using EDM" on page 451.

The maximum number of columns that a single data source file can have is 32. If the data source file has more than 32 columns, the Enforce Server administration console produces an error message at the profile screen, and the data source file is not indexed. There is no maximum number of rows, but the total number of cells in a single data source file should not exceed 2.1 billion cells. If your data source file is larger than this, split it into multiple files and index each separately.

Table 19-1 summarizes size limitations for FDM data source files.

Note: The format for the data source file should be a text-based format containing pipe- or tab-delimited contents. In general you should avoid using a spreadsheet format for the data source file (such as XLS or XLSX) because such programs use use scientific notation to render numbers.

Data source file	Limit	Description
Columns	32	The data source file cannot have more than 32 columns. If it does, the system does not index it.
Cells	2.1 billion	The data source file cannot have more than 2.1 billion data cells. If it does, the system does not index it.
Rows	None	There is no limit to the number of rows that the data source file can have as long as the column and cell limitations are adhered to.

**Table 19-1** EDM data source file size limitations

### About cleansing the exact data source file

Once you have created the data source file, you must prepare the data for indexing by cleansing it. It is critical that you cleanse the data source file to ensure that your EDM policies are as accurate as possible. You can use tools such as Stream Editor (sed) and AWK to cleanse the data source file. Melissa Data provides good tools for normalizing data in the data source, such as addresses.

See Table 19-2 on page 373. provides the workflow for cleansing the data source file for indexing.

**Table 19-2** Workflow for cleansing the data source file

Step	Action	Description
1	Prepare the data source file for indexing.	See "Preparing the exact data source file for indexing" on page 381.
2	Ensure that the data source has at least one column that is unique data.	See "Ensure data source has at least one column of unique data" on page 452.
3	Remove incomplete and duplicate records. Do not fill empty cells with bogus data.	See "Cleanse the data source file of blank columns and duplicate rows" on page 453.
4	Remove improper characters.	See "Remove ambiguous character types from the data source file" on page 454.
5	Verify that the data source file is below the error threshold.	

#### About using System Fields for data source validation

Column headings in your data source are useful for visual reference. However, they do not tell Symantec Data Loss Prevention what kind of data the columns contain. To do this, you use the Field Mappings section of the Exact Data Profile to specify mappings between fields in your data source. You can also use field mappings to specify fields that the system recognizes in the system-provided policy templates. The Field Mappings section also gives you advanced options for specifying custom fields and validating the data in those fields.

See "Mapping Exact Data Profile fields" on page 389.

Consider the following example use of field mappings. Your company wants to protect employee data, including employee social security numbers. You create a Data Loss Prevention policy based on the Employee Data Protection template. The policy requires an exact data index with fields for social security numbers and other employee data. You prepare your data source and then create the Exact Data **Profile**. To validate the data in the social security number field, you map this column field in your index to the "Social Security Number" system field pattern. The system will then validate all data in that field using the Social Security Number validator to ensure that each data item is a social security number

Using the system-defined field patterns to validate your data is critical to the accuracy of your EDM policies. If there is no system-defined field pattern that corresponds to one or more data fields in your index, you can define custom fields and choose the appropriate validator to validate the data.

See "Map data source column to system fields to leverage validation" on page 455.

#### About index scheduling

After you have indexed an exact data source extract, its schema cannot be changed because the \*.rdx index file is binary. If the data source changes, or the number of columns or data mapping of the exact data source file changes, you must create a new EDM index and update the policies that reference the changed data. In this case you can schedule the indexing to keep the index in sync with the data source.

The typical use case is as follows. You extract data from a database to a file and cleanse it. This is your data source file. Using the Enforce Server administration console you define an Exact Data Profile and index the data source file. The system generates the \*.rdx index file and deploys it to one or more detection servers. However, you know that the data changes frequently and you will need to generate a new data source file weekly or monthly to keep up with the changes to the database. In this case you can use index scheduling so that you can automate the indexing of the data source file so you do not have to return to the Enforce Server administration console and reindex the updated data source. Your only task is to

drop an updated and cleansed data source file to the Enforce Server for scheduled indexing.

See "Configuring Exact Data profiles" on page 378.

See "Scheduling Exact Data Profile indexing" on page 392.

See "Use scheduled indexing to automate profile updates" on page 457.

#### About the Content Matches Exact Data From condition

The Content Matches Exact Data From an Exact Data Profile condition is the detection component you use to implement EDM policies. When you define this condition, you select the EDM profile on which the condition is based. You also select the rows you want to use in your condition, as well as any WHERE clause limitations.

Note: You cannot use the Content Matches Exact Data From an Exact Data Profile condition as a policy exception. Data Loss Prevention does not support the use of the EDM condition as a policy exception.

See "Configuring the Content Matches Exact Data policy condition" on page 396.

### **About Data Owner Exception**

Although EDM does not support the explicit use of match exceptions in policies, EDM does support criteria-based matching exceptions. This feature of EDM is known as Data Owner Exception. Data owner exception lets you tag or authorize a specific field in an Exact Data Profile as the data owner. At run-time if the sender or recipient of the data is authorized as a data owner, the condition does not trigger a match and the data is allowed to be sent or received by the data owner

You implement data owner exception by including either the email address field or domain address field in your Exact Data Profile. In the EDM policy condition, you specify the field as either the sender or recipient data owner. An authorized data owner, identified by his or her email address or a domain address, who is a sender can send his or her own confidential information without triggering an EDM match or incident. This means that the sender can send any information that is contained in the row where his or her email address or domain is specified. Authorized data owner recipients can be specified individually or all recipients in the list can be allowed to receive the data without triggering a match.

As a policy author, data owner exception gives you the flexibility to allow data owners to use their own data legitimately. For example, if data owner exception is enabled, an employee can send an email containing his or her own confidential information

(such as an account number) without triggering a match or an incident. Similarly, if data owner exception is configured for a recipient, the system does not trigger an EDM match or incident if the data owner is receiving his or her own information, such as someone outside the company is sending a email to the data owner containing his or her account number.

See "About upgrading EDM deployments" on page 377.

See "Creating the exact data source file for Data Owner Exception" on page 380.

See "Configuring Data Owner Exception for EDM policy conditions" on page 398.

### About profiled Directory Group Matching (DGM)

Profiled Directory Group Matching (DGM) is a specialized implementation of EDM that is used to detect the exact identity of a message user, sender, or recipient that has been profiled from a directory server or database

Profiled DGM leverages EDM technology to detect identities that you have indexed from your database or directory server using an Exact Data Profile. For example, you can use profiled DGM to identify network user activity or to analyze content associated with particular users, senders, or recipients. Or, you can exclude certain email addresses from analysis. Or, you might want to prevent certain people from sending confidential information by email.

To implement profiled DGM, your exact data source file must contain one or more of the following fields:

- Fmail address
- IP address
- Windows user name
- IM name (AOL, Yahoo, MSN)

If you include the email address field in the DGM profile, the field will appear in the Directory EDM drop-down list at the incident snapshot screen in the Enforce Server administration console, which facilitates remediation.

See "Creating the exact data source file for profiled DGM" on page 380.

See "Include an email address field in the Exact Data Profile for profiled DGM" on page 461.

See "Use profiled DGM for Network Prevent for Web identity detection" on page 461.

#### About two-tier detection for EDM on the endpoint

The EDM index is server-based. If you deploy a policy containing an EDM condition to the DLP Agent on the endpoint, the system uses two-tier detection to evaluate data for matching. In this case the EDM detection condition is not evaluated locally by the DLP Agent. Instead, the DLP Agent sends the data to the Endpoint Server for evaluation against the index. If the endpoint is offline, the message cannot be sent until the server is available, which can affect endpoint performance.

See "Two-tier detection for DLP Agents" on page 309.

To check if two-tier detection is being used, check the

\SymantecDLP\Protect\logs\debug\FileReader.log on the Endpoint Server to see if any EDM indexes are being loaded. Look for the line "loaded database profile."

See "Troubleshooting policies" on page 353.

### About upgrading EDM deployments

Symantec Data Loss Prevention version 12.5 provides several enhancements to EDM, including support for multi-token cell indexing and proportional proximity range checking. Refer to the following document for an overview of these enhancements: What's New and What's Changed in Symantec Data Loss Prevention Version 12.5.

To take advantage of these EDM enhancements, you must upgrade your servers to Symantec Data Loss Prevention version 12.5 and you must reindex your EDM data sources using the 12.5 EDM Indexer. Although legacy EDM indexes will run on 12.5 detection servers, such indexes do support new features. In addition, you must calculate the memory required to index the data source and load and process each EDM index at run-time.

In addition, if you have previously implemented data owner exceptions manually using configuration files, you must reconfigure these exceptions using the Enforce Server administration console. Refer to the following article at the DLP Knowledgebase for instructions on migrating legacy DOE configurations to the Enforce Server 12.x platform: https://kb-vontu.altiris.com/article.asp?article=56307.

See "About Data Owner Exception" on page 375.

See "Updating EDM indexes to version 12.5" on page 416.

See "Memory requirements for EDM" on page 421.

See "EDM index out of date error codes" on page 420.

## **Configuring Exact Data profiles**

To implement EDM, you create the **Exact Data Profile**, index the data source, and define one or more EDM detection conditions to match profiled data exactly.

See "About the Exact Data Profile and index" on page 371.

**Table 19-3** Implementing Exact Data Matching

Step	Action	Description
1	Create the data source file.	Export the source data from the database (or other data repository) to a tabular text file.
		If you want to except data owners from matching, you need to include specific data items in the data source file.
		See "About the exact data source file" on page 372.
		If you want to match identities for profiled Directory Group Matching (DGM), you need to include specific data items in the data source files.
		See "Creating the exact data source file for EDM" on page 379.
2	Prepare the data source file for	Remove irregularities from the data source file.
	indexing.	See "Preparing the exact data source file for indexing" on page 381.
3	Upload the data source file to the Enforce Server.	You can copy or upload the data source file to the Enforce Server, or access it remotely.
		See "Uploading exact data source files to the Enforce Server" on page 383.
4	Create an Exact Data Profile.	An Exact Data Profile is required to implement Exact Data Matching (EDM) policies. The Exact Data Profile specifies the data source, data field types, and the indexing schedule.
		See "Creating and modifying Exact Data Profiles" on page 385.
5	Map and validate the data fields.	You map the source data fields to system or custom data types that the system validates. For example, a social security number data field needs to be nine digits.
		See "About using System Fields for data source validation" on page 374.
		See "Mapping Exact Data Profile fields" on page 389.
6	Index the data source, or	See "About index scheduling" on page 374.
	schedule indexing.	See "Scheduling Exact Data Profile indexing" on page 392.

Step	Action	Description
7	Configure and tune one or more EDM detection conditions.	See "Configuring the Content Matches Exact Data policy condition" on page 396.
		See "Configuring the Content Matches Exact Data policy condition" on page 396.

**Table 19-3** Implementing Exact Data Matching (continued)

#### Creating the exact data source file for EDM

The first step in the EDM indexing process is to create the data source. A data source is a flat file containing data in a standard delimited format.

If you plan to use a policy template, review it before creating the data source file to see which data fields the policy uses. For relatively small data sources, include as many suggested fields in your data source as possible. However, note that the more fields you include, the more memory the resulting index requires. This consideration is important if you have a large data source. When you create the data profile, you can confirm how well the fields in your data source match against the suggested fields for the template.

See Table 19-4 on page 379.

Create the exact data source file Table 19-4

Step	Description
1	Export the data you want to protect from a database or other tabular data format, such as an Excel spreadsheet, to a flat file. The data source file you create must be a tabular text file that contains rows of data from the original source. Each row from the original source is included as a row in the data source file. Delimit columns using a tab, a comma, or a pipe. Pipe is preferred. Comma should not be used if your data source fields contain numbers.
	See "About the exact data source file" on page 372.
	You must maintain all the structured data that you exported from the source database table or table-like format in one data source file. You cannot split the data source across multiple files.
	The data source file cannot exceed 32 columns or 2.1 billion cells. The size of a data source file is otherwise limited only by the available disk space of the Enforce Server host. If you plan to upload the data source file to the Enforce Server, browser capacity limits the data source size to 2 GB. For file sizes larger than this size you can copy the file to the Enforce Server using FTP/S.

Description Step 2 Include required data fields for specific EDM implementations: Unique data For all EDM implementations, make sure the data source contains at least one column of unique See "Ensure data source has at least one column of unique data" on page 452. Data Owner Exception Make sure the data source contains the email address field or domain field, if you plan to use data owner exceptions. See "Creating the exact data source file for Data Owner Exception" on page 380. Directory Group Matching Make sure the data source includes one or more sender/recipient identifying fields. See "Creating the exact data source file for profiled DGM" on page 380. 3 Prepare the data source file for indexing.

**Table 19-4** Create the exact data source file (continued)

#### Creating the exact data source file for Data Owner Exception

See "Preparing the exact data source file for indexing" on page 381.

To implement Data Owner Exception and ignore data owners from detection, you must explicitly include each user's email address or domain address in the Exact Data Profile. Each expected domain (for example, symantec.com) must be explicitly added to the Exact Data Profile. The system does not automatically match on subdomains (for example, fileconnect.symantec.com). Each subdomain must be explicitly added to the Exact Data Profile.

To implement the data owner exception feature, you must include either or both of the following fields in your data source file:

- Email address
- Domain address

See "About Data Owner Exception" on page 375.

See "Configuring Data Owner Exception for EDM policy conditions" on page 398.

### Creating the exact data source file for profiled DGM

Profiled DGM leverages Exact Data Matching (EDM) technology to precisely detect identities. Identity-related attributes may include an IP address, email address, user name, business unit, department, manager, title, or employment status. Other attributes may be whether that employee has provided consent to be monitored,

or whether the employee has access to sensitive information. To implement profiled DGM, you must include at least one required data field in your data source.

See "About the Exact Data Profile and index" on page 371.

Table 19-5 lists the required fields for profiled DGM. The data source file must contain at least one of these fields.

Profiled DGM data source fields **Table 19-5** 

Field	Description	
Email address	If you use an email address column filed in the data source file, the email address appears in the <b>Directory EDM</b> drop-down list at the incident snapshot screen.	
IP address	For example: 172.24.56.33	
Windows user name	If you use a Windows user name field in your data source, the data must be in the following format: domain\user; for example: ACME\john_smith.	
AOL IM name	IM screen name / handle	
Yahoo! IM name	For example: myhandle123	
MSN IM name		

### Preparing the exact data source file for indexing

Once you create the exact data source file, you must prepare it so that you can efficiently index the data you want to protect.

When you index an exact data profile, the Enforce Server keeps track of empty cells and any misplaced data which count as errors. For example, an error may be a name that appears in a column for phone numbers. Errors can constitute a certain percentage of the data in the profile (five percent, by default). If this default error threshold is met, Symantec Data Loss Prevention stops indexing. It then displays an error to warn you that your data may be unorganized or corrupt. Symantec Data Loss Prevention checks for errors only if the data source has at least a thousand rows.

#### To prepare the exact data source for EDM indexing

- Make sure that the data source file is formatted as follows:
  - If the data source has more than 200,000 rows, verify that it has at least two columns of data. One of the columns should contain unique values. For example, credit card numbers, driver's license numbers, or account numbers (as opposed to first and last names, which are generic).

See "Ensure data source has at least one column of unique data" on page 452.

- Verify that you have delimited the data source using pipes ( | ) or tabs. If the data source file uses commas as delimiters, remove any commas that do not serve as delimiters.
  - See "Do not use the comma delimiter if the data source has number fields" on page 455.
- Verify that data values are not enclosed in quotes.
- Remove single-character and abbreviated data values from the data source. For example, remove the column name and all values for a column in which the possible values are Y and N. Optionally, remove any columns that contain numeric values with less that five digits, as these can cause false positives in production.
  - See "Remove ambiguous character types from the data source file" on page 454.
- Verify that numbers, such as credit card or social security, are delimited internally by dashes, or spaces, or none at all. Make sure that you do not use a data-field delimiter such as a comma as an internal delimiter in any such numbers. For example: 123-45-6789, or 123 45 6789, or 123456789 are valid, but not 123,45,6789.
  - See "Do not use the comma delimiter if the data source has number fields" on page 455.
- Eliminate duplicate records, which can cause duplicate incidents in production.
  - See "Cleanse the data source file of blank columns and duplicate rows" on page 453.
- Do not index common values. EDM works best with values that are unique. Think about the data you want to index (and thus protect). Is this data truly valuable? If the value is something common, it is not useful as an EDM value. For example, suppose you want to look for "US states." Since there are only 50 states, if your exact data profile has 300,000 rows, the result is a lot of duplicates of common values. Symantec Data Loss Prevention indexes all values in the exact data profile, regardless of if the data is used in a policy or not. It is good practice to use values that are less common and preferably unique to get the best results with EDM.

See "Ensure data source has at least one column of unique data" on page 452.

2 Once you have prepared the exact data source file, proceed with the next step in the EDM process: upload the exact data source file to the Enforce Server for profiling the data you want to protect.

See "Uploading exact data source files to the Enforce Server" on page 383.

### Uploading exact data source files to the Enforce Server

After you have prepared the data source file for indexing, load it to the Enforce Server so the data source can be indexed.

See "Creating and modifying Exact Data Profiles" on page 385.

Listed here are the options you have for making the data source file available to the Enforce Server. Consult with your database administrator to determine the best method for your needs.

**Table 19-6** Uploading the data source file to the Enforce Server for indexing

Upload option(s)	Use case	Description
Upload Data Source to Server Now	Data source file is less than 50 MB	If you have a smaller data source file (less than 50 MB), upload the data source file to the Enforce Server using the Enforce Server administration console (web interface). When creating the <b>Exact Data Profile</b> , you can specify the file path or browse to the directory and upload the data source file.
		<b>Note:</b> Due to browser capacity limits, the maximum file size that you can upload is 2 GB. However, uploading any file over 50 MB is not recommended since files over this size can take a long time to upload. If your data source file is over 50 MB, consider copying the data source file to the datafiles directory using the next option.

Uploading the data source file to the Enforce Server for indexing **Table 19-6** (continued)

\		
Upload option(s)	Use case	Description
Reference Data Source on Manager Host	Data source file is over 50 MB	If you have a large data source file (over 50 MB), copy it to the ${\tt datafiles}$ directory on the host where Enforce is installed.
		<ul> <li>On Windows this directory is located at \SymantecDLP\Protect\datafiles.</li> <li>On Linux this directory is located at /var/SymantecDLP/datafiles.</li> </ul>
		This option is convenient because it makes the data file available by reference by a drop-down list during configuration of the <b>Exact Data Profile</b> . If it is a large file, use a third-party solution (such as Secure FTP) to transfer the data source file to the Enforce Server.
		<b>Note:</b> Ensure that the Enforce user (usually called "protect") has <b>modify</b> permissions (on Windows) or <b>rw</b> permissions (on Linux) for all files in the datafiles <b>directory</b> .
Use This File Name	Data source file is not yet created	In some cases you may want to create an EDM profile before you have created the data source file. In this case you can create a profile template and specify the name of the data source file you plan to create. This option lets you define EDM policies using the EDM profile template before you index the data source. The policies do not operate until the data source is indexed. When you have created the data source file you place it in the \SymantecDLP\Protect\datafiles directory and index the data source immediately on save or schedule indexing.
		See "Creating and modifying Exact Data Profiles" on page 385.

Table 19-6	Uploading the data source file to the Enforce Server for indexing
	(continued)

Upload option(s)	Use case	Description
and be rei	Data source is to be indexed remotely and copied to the Enforce Server	In some environments it may not be secure or feasible to copy or upload the data source file to the Enforce Server. In this situation you can index the data source remotely using Remote EDM Indexer.  See "Remote EDM indexing" on page 432.  This utility lets you index an exact data source on a computer other than the Enforce Server host. This feature is useful when you do not want to copy the data source file to the same computer as the Enforce Server. As an example, consider a situation where the originating department wants to avoid the security risk of copying the data to an extra-departmental host. In this case you can use the Remote EDM
		First you create an EDM profile template where you choose the <b>Use this File Name</b> and the <b>Number of Columns</b> options. You must specify the name of the data source file and the number of columns it contains.  See "Creating an EDM profile template for remote indexing" on page 436. You then use the Remote EDM Indexer to remotely index the data source and copy the index files to the Enforce Server host and load the externally generated index. The <b>Load Externally Generated Index</b> option is only available after you have defined and saved the profile. Remote indexes are loaded from the /SymantecDLP/Protect/Index directory on the Enforce Server host.  See "Copying and loading remote index files to the Enforce Server" on page 442.

### Creating and modifying Exact Data Profiles

The Manage > Data Profiles > Exact Data > Add Exact Data Profile screen is the home page for managing and adding Exact Data Profiles. An Exact Data Profile is required to implement an instance of the Content Matches Exact Data detection rule. An Exact Data Profile specifies the data source, the indexing parameters, and the indexing schedule. Once you have created the EDM profile, you index the data source and configure one or more detection rules to use the profile and detect exact content matches

See "Configuring Exact Data profiles" on page 378.

Note: If you are using the Remote EDM Indexer to generate the Exact Data Profile, refer to the following topic.

#### To create or modify an Exact Data Profile

- 1 Make sure that you have created the data source file.
  - See "Creating the exact data source file for EDM" on page 379.
- 2 Make sure that you have prepared the data source file for indexing.
  - See "Preparing the exact data source file for indexing" on page 381.
- 3 Make sure the data source contains the email address field or domain field, if you plan to use data owner exceptions.
  - See "About Data Owner Exception" on page 375.
- In the Enforce Server administration console, navigate to **Manage > Data** Profiles > Exact Data.
- 5 Click Add Exact Data Profile.
- Enter a unique, descriptive **Name** for the profile (limited to 256 characters). 6
  - For easy reference, choose a name that describes the data content and the index type (for example, Employee Data EDM).
  - If you modify an existing Exact Data Profile you can change the profile name.
- Select one of the following **Data Source** options to make the data source file available to the Enforce Server:

#### Upload Data Source to Server Now

If you are creating a new profile, click **Browse** and select the data source file, or enter the full path to the data source file.

If you are modifying an existing profile, select **Upload Now**.

See "Uploading exact data source files to the Enforce Server" on page 383.

#### Reference Data Source on Manager Host

If you copied the data source file to the "datafiles" directory on the Enforce Server, it appears in the drop-down list for selection.

See "Uploading exact data source files to the Enforce Server" on page 383.

#### Use This File Name

Select this option if you have not yet created the data source file but want to configure EDM policies using a placeholder EDM profile. Enter the file name of the data source you plan to create, including the Number of **Columns** it is to have. When you do create the data source, you must copy it to the "datafiles" directory.

See "Uploading exact data source files to the Enforce Server" on page 383.

Note: Use this option with caution. Be sure to remember to create the data source file and copy it to the "datafiles" directory. Name the data source file exactly the same as the name you enter here and include the exact number of columns you specify here.

#### Load Externally Generated Index

Select this option if you have created an index on a remote computer using the Remote EDM Indexer. This option is only available after you have defined and saved the profile. Profiles are loaded from the /SymantecDLP/Protect/Index directory on the Enforce Server host. See "Uploading exact data source files to the Enforce Server" on page 383.

- 8 If the first row of your data source contains Column Names, select the "Read first row as column names" check box.
- 9 Specify the **Error Threshold**, which is the maximum percentage of rows that contain errors before indexing stops.

A data source error is either an empty cell, a cell with the wrong type of data, or extra cells in the data source. For example, a name in a column for phone numbers is an error. If errors exceed a certain percentage of the overall data source (by default, 5%), the system guits indexing and displays an indexing error message. The index is not created if the data source has more invalid records than the error threshold value allows. Although you can change the threshold value, more than a small percentage of errors in the data source can indicate that the data source is corrupt, is in an incorrect format, or cannot be read. If you have a significant percentage of errors (10% or more), stop indexing and cleanse the data source.

See "Preparing the exact data source file for indexing" on page 381.

- 10 Select the Column Separator Char (delimiter) that you have used to separate the values in the data source file. The delimiters you can use are tabs, commas, or pipes.
- 11 Select one of the following encoding values for the content to analyze, which must match the encoding of your data source:
  - ISO-8859-1 (Latin-1) (default value) Standard 8-bit encoding for Western European languages using the Latin alphabet.

#### ■ UTF-8

Use this encoding for all languages that use the Unicode 4.0 standard (all single- and double-byte characters), including those in East Asian languages.

#### UTF-16

Use this encoding for all languages that use the Unicode 4.0 standard (all single- and double-byte characters), including those in East Asian languages.

Note: Make sure that you select the correct encoding. The system does not prevent you from creating an EDM profile using the wrong encoding. The system only reports an error at run-time when the EDM policy attempts to match inbound data. To make sure that you select the correct encoding, after you clickNext, verify that the column names appear correctly. If the column names do not look correct, you chose the wrong encoding.

- 12 Click Next to go to the second Add Exact Data Profile screen.
- 13 The Field Mappings section displays the columns in the data source and the field to which each column is mapped in the Exact Data Profile. Field mappings in existing Exact Data Profiles are fixed and, therefore, are not editable.

See "About using System Fields for data source validation" on page 374.

See "Mapping Exact Data Profile fields" on page 389.

Confirm that the column names in your data source are accurately represented in the Data Source Field column. If you selected the Column Names option, the Data Source Field column lists the names in the first row of your data source. If you did not select the Column Names option, the column lists Col 1, Col 2, and so on.

14 In the System Field column, select a field from the drop-down list for each data source field. (This step is required if you use a policy template, or if you want to check for errors in the data source.)

For example, for a data source field that is called SOCIAL SECURITY NUMBER, select Social Security Number from the corresponding drop-down list. The values in the System Field drop-down lists include all suggested fields for all policy templates.

- 15 Optionally, specify and name any custom fields (that is, the fields that are not pre-populated in the **System Field** drop-down lists). To do so, perform these steps in the following order:
  - Click Advanced View to the right of the Field Mappings heading. This screen displays two additional columns (Custom Name and Type).
  - To add a custom system field name, go to the appropriate System Field drop-down list. Select Custom, and type the name in the corresponding Custom Name text field.

- To specify a pattern type (for purposes of error checking), go to the appropriate Type drop-down list and select the wanted pattern. (To see descriptions of all available pattern types, click **Description** at the top of the column.)
- 16 Check your field mappings against the suggested fields for the policy template you plan to use. To do so, go to the Check Mappings Against drop-down list, select a template, and click Check now on the right.

The system displays a list of all template fields that you have not mapped. You can go back and map these fields now. Alternatively, you may want to expand your data source to include as many expected fields as possible, and then re-create the exact data profile. Symantec recommends that you include as many expected data fields as possible.

- 17 In the Indexing section of the screen, select one of the following options:
  - Submit Indexing Job on Save

Select this option to begin indexing the data source when you save the exact data profile.

#### Submit Indexing Job on Schedule

Select this option to index the data source according to a specific schedule. Make a selection from the **Schedule** drop-down list and specify days, dates, and times as required.

See "About index scheduling" on page 374.

See "Scheduling Exact Data Profile indexing" on page 392.

#### 18 Click Finish.

After Symantec Data Loss Prevention finishes indexing, it deletes the original data source from the Enforce Server. After you index a data source, you cannot change its schema. If you change column mappings for a data source after you index it, you must create a new exact data profile.

After the indexing process is complete you can create new EDM rules for your policies that reference the Exact Data Profile you have created.

See "Configuring the Content Matches Exact Data policy condition" on page 396.

#### Mapping Exact Data Profile fields

After you have added and configured the data source file and settings, the Manage > Data Profiles > Exact Data > Add Exact Data Profile screen lets you map the fields from the data source file to the Exact Data Profile you configure.

To enable error checking on a field in a data source or to use the index with a policy template that uses a system field, you must map the field in the data source to the system field. The Field Mappings section lets you map the columns in the original data source to system fields in the Exact Data Profile.

**Table 19-7** Field mapping options

Field	Description
Data Source Field	If you selected the Column Names option at the Add Exact Data Profile screen, this column lists the values that are found in the first row from the data source. If you did not select this option, this column lists the columns by generic names (such as Col 1, Col 2, and so on).
	<b>Note:</b> If you are implementing data owner exception, you must map either or both the email address and domain fields.
	See "Configuring the Content Matches Exact Data policy condition" on page 396.
System Field	Select the system field for each column.
	A system field value (except <b>None Selected</b> ) cannot be mapped to more than one column.
	Some system fields have system patterns associated with them (such as social security number) and some do not (such as last name).
	See "Using system-provided pattern validators for EDM profiles" on page 391.
Check mappings against policy	Select a policy template from the drop-down list to compare the field mappings against and then click <b>Check now</b> .
template	All policy templates that implement EDM appear in the drop-down menu, including any you have imported.
	See "Choosing an Exact Data Profile" on page 322.
	If you plan to use more than one policy template, select one and check it, and then select another and check it, and so on.
	If there are any fields in the policy template for which no data exists in the data source, a message appears listing the missing fields. You can save the profile anyway or use a different Exact Data Profile.
Advanced View	If you want to customize the schema for the exact data profile, click <b>Advanced View</b> to display the advanced field mapping options.
	Table 19-8 lists and describes the additional columns you can specify in the <b>Advanced View</b> screen.
Indexing	Select one of the indexing options.
	See "Scheduling Exact Data Profile indexing" on page 392.
Finish	Click <b>Finish</b> when you are done configuring the Exact Data Profile.

From the **Advanced View** you map the system and data source fields to system patterns. System patterns map the specified structure to the data in the Exact Data Profile and enable efficient error checking and hints for the indexer.

**Table 19-8 Advanced View options** 

Field	Description	
Custom Name	If you select Custom Name for a System Field, enter a unique name for it and then select a value for Type. The name is limited to 60 characters.	
Туре	If you select a value other than Custom for a System Field, some data types automatically select a value for Type. For example, if you select <b>Birth Date</b> for the System Field, <b>Date</b> is automatically selected as the Type. You can accept it or change it.	
	Some data types do not automatically select a value for Type. For example, if you select <b>Account Number</b> for the System Field, the Type remains unselected. You can specify the data type of your particular account numbers.	
	See "Using system-provided pattern validators for EDM profiles" on page 391.	
Description	Click the link (description) beside the Type column header to display a pop-up window containing the available system data types. See also the topic link below.	
	See "Using system-provided pattern validators for EDM profiles" on page 391.	
Simple View	Click <b>Simple View</b> to return to the Simple View (with the Custom Name and Type columns hidden).	

See "Creating and modifying Exact Data Profiles" on page 385.

### Using system-provided pattern validators for EDM profiles

Table 19-9 lists and describes the system-provided data validators for EDM profiles.

System-provided data validators for EDM profiles **Table 19-9** 

Туре	Description
Credit Card Number	The Credit Card pattern is built around knowledge about various internationally recognized credit cards, their registered prefixes, and number of digits in account numbers. The following types of Credit Cards patterns are validated: MasterCard, Visa, America Express, Diners Club, Discover, Enroute, and JCB.
	Optional spaces in designated areas within credit cards numbers are recognized. Note that only spaces in generally accepted locations (for example, after every 4th digit in MC/Visa) are recognized. Note that the possible location of spaces differs for different card types. Credit card numbers are validated using checksum algorithm. If a number looks like a credit card number (that is, it has correct number of digits and correct prefix), but does not pass checksum algorithm, it is not considered to be a credit card, but just a number.

**Table 19-9** System-provided data validators for EDM profiles (continued)

Туре	Description	
Email	Email is a sequence of characters that looks like the following: string@string.tld, where string may contain letters, digits, underscore, dash, and dot, and 'tld' is one of the approved DNS top level generic domains, or any two letters (for country domains).	
IP Address	IP Address is a collection of 4 sequences of between 1 and 3 digits, separated by dots.	
Number	Number is either float or integer, either by itself or in round brackets (parenthesis).	
Percent	Percent is a number immediately followed by the percent sign ("%"). No space is allowed between a number and a percent sign.	
Phone	Only US and Canadian telephone numbers are recognized. The phone number must start with any digit but 1, with the exception of numbers that include a country code	
	Phone number can be one of the following formats:	
	<ul> <li>7 digits (no spaces or dashes)</li> <li>Same as above, preceded by 3 digits, or by 3 digits in round brackets, followed by spaces or dashes</li> </ul>	
	<ul> <li>3 digits, followed by optional spaces/dashes, followed by 4 digits</li> <li>Same as above, preceded by the number 1, followed by spaces or dashes</li> </ul>	
	All cases above can be optionally followed by an extension number, preceded by spaces or dashes. The extension number is 2 to 5 digits preceded by any of the following (case insensitive): 'x' 'ext' 'exten' 'extens' 'extensions' optionally followed by a dot and spaces.	
	<b>Note:</b> The system does not recognize the pattern XXX-XXX-XXX as a valid phone number format because this format is frequently used in other forms of identification. If your data source contains a column of phone numbers in that format, select <b>None Selected</b> to avoid confusion between phone numbers and other data.	
Postal Code	Only US ZIP codes and Canadian Postal Codes are recognized. The US ZIP code is a sequence of 5 digits, optionally followed by dash, followed by another 4 digits. The Canadian Postal Code is a sequence like K2B 8C8, that is, "letter-digit-letter-space-digit-letter-digit" where space(s) in the middle is optional.	
Social Security Number	Only US TAX IDs are recognized. The TAX ID is a 3 digits, optionally followed by spaces or dashes, followed by 2 digits, optionally followed by spaces or dashes, followed by 4 digits.	

## Scheduling Exact Data Profile indexing

When you configure an Exact Data Profile, you can set a schedule for indexing the data source (Submit Indexing on Job Schedule).

See "About index scheduling" on page 374.

Before you set up a schedule, consider the following recommendations:

- If you update your data sources occasionally (for example, less than once a month), there is no need to create a schedule. Index the data each time you update the data source.
- Schedule indexing for times of minimal system use. Indexing affects performance throughout the Symantec Data Loss Prevention system, and large data sources can take time to index.
- Index a data source as soon as you add or modify the corresponding exact data profile, and re-index the data source whenever you update it. For example, consider a scenario whereby every Wednesday at 2:00 A.M. you update the data source. In this case you should schedule indexing every Wednesday at 3:00 A.M. Do not index data sources daily as this can degrade performance.
- Monitor results and modify your indexing schedule accordingly. If performance is good and you want more timely updates, for example, schedule more frequent data updates and indexing.

The Indexing section lets you index the Exact Data Profile as soon as you save it (recommended) or on a regular schedule as follows:

Table 19-10 Scheduling indexing for Exact Data Profiles

Parameter	Description
Submit Indexing Job on Save	Select this option to index the Exact Data Profile when you click Save.
Submit Indexing Job on Schedule	Select this option to schedule an indexing job. The default option is <b>No Regular Schedule</b> . If you want to index according to a schedule, select a desired schedule period, as described.
Index Once	On – Enter the date to index the document profile in the format MM/DD/YY. You can also click the date widget and select a date.
	At – Select the hour to start indexing.
Index Daily	At – Select the hour to start indexing.
	<b>Until</b> – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.
Index Weekly	Day of the week – Select the day(s) to index the document profile.
	At – Select the hour to start indexing.
	Until – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.

Table 19-10	Scheduling indexing	for Exact Data Profiles	(continued)
-------------	---------------------	-------------------------	-------------

Parameter	Description
Index Monthly	Day – Enter the number of the day of each month you want the indexing to occur. The number must be 1 through 28.
	At – Select the hour to start indexing.
	Until – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.

See "Mapping Exact Data Profile fields" on page 389.

See "Creating and modifying Exact Data Profiles" on page 385.

### Managing and adding Exact Data Profiles

You manage and create Exact Data Profiles for EDM at the Manage > Data Profiles > Exact Data screen. Once a profile has been created, the Exact Data screen lists all Exact Data Profiles configured in the system.

See "About the Exact Data Profile and index" on page 371.

Table 19-11 **Exact Data screen actions** 

Action	Description	
Add EDM profile	Click Add Exact Data Profile to define a new Exact Data Profile.	
	See "Configuring Exact Data profiles" on page 378.	
Edit EDM profile	To modify an existing <b>Exact Data Profile</b> , click the name of the profile, or click the pencil icon at the far right of the profile row.	
	See "Creating and modifying Exact Data Profiles" on page 385.	
Remove EDM profile	Click the red X icon at the far right of the profile row to delete the Exact Data Profile from the system. A dialog box confirms the deletion.	
	<b>Note:</b> You cannot edit or remove a profile if another user currently modifies that profile, or if a policy exists that depends on that profile.	
Download EDM profile	Click the download profile link to download and save the Exact Data Profile.	
	This is useful for archiving and sharing profiles across environments. The file is in the binary *.edm format.	

Table 19-11 Exact Data screen actions (continued)

Action	Description
Refresh EDM profile status	Click the refresh arrow icon at the upper right of the <b>Exact Data</b> screen to fetch the latest status of the indexing process.
	If you are in the process of indexing, the system displays the message "Indexing is starting." The system does not automatically refresh the screen when the indexing process completes.

Table 19-12 Exact Data screen details

Column	Description	
Exact Data Profile	The name of the exact data profile.	
Last Active Version	ctive Version The version of the exact data profile and the name of the detection server that runs the profile	
Status	The current status of the exact data profile, which can be any of the following:  Next scheduled indexing (if it is not currently indexing)  Sending an index to a detection server  Indexing  Deploying to servers  In addition, the current status of the indexing process for each detection server, which can be any of the following:  Completed, including a completion date  Pending index completion (waiting for the Enforce Server to finish indexing the exact data source file)  Replicating indexing  Creating index (internally)	
	Building caches	
Error messages	The <b>Exact Data</b> screen displays any error messages in red.  For example, if the Exact Data Profile is corrupt or does not exist, the system displays an error	
	message.	

## **Configuring EDM policies**

This section describes how to configure EDM policy conditions.

See "Configuring the Content Matches Exact Data policy condition" on page 396.

See "Configuring Data Owner Exception for EDM policy conditions" on page 398.

See "Configuring the Sender/User based on a Profiled Directory policy condition" on page 399.

See "Configuring the Recipient based on a Profiled Directory policy condition" on page 399.

See "Configuring Advanced Server Settings for EDM policies" on page 400.

### Configuring the Content Matches Exact Data policy condition

Once you have defined the Exact Data Profile and indexed the data source, you configure one or more Content Matches Exact Data conditions in policy rules

See "About the Content Matches Exact Data From condition" on page 375.

Table 19-13 Configure the Content Matches Exact Data policy condition

Steps	Action	Description
1	Configure an EDM policy detection rule.	Create a new EDM detection rule in a policy, or modify an existing EDM rule.
		See "Configuring policies" on page 326.
		See "Configuring policy rules" on page 330.
Match Data Rows when All of these match		
2	Select the fields to match.	The first thing you do when configuring the EDM condition is select each data field that you want the condition to match. You can <b>select all</b> or <b>deselect all</b> fields at once. The system displays all the fields or columns that were included in the index. You do not have to select all the fields, but you should select at least 2 or 3, one of which must be unique, such as social security number, credit card number, and so forth.  See "Best practices for using EDM" on page 451.
3	Choose the number of selected fields to match.	Choose the number of the selected fields to match from the drop down menu. This number represents the number of fields of those selected that must be present in a message to trigger a match. You must select at least as many fields to match as the number of data fields you check. For example, if you choose 2 of the selected fields from the menu, you must have checked at least two fields present in a message for detection.  See "Ensure data source has at least one column of unique data" on page 452.

Configure the Content Matches Exact Data policy condition **Table 19-13** (continued)

Steps	Action	Description			
4	Select the WHERE clause to enter specific field values to match (optional).	The <b>WHERE</b> clause option matches on the specified field value. You specify a WHERE clause value by selecting an exact data field from the menu and by entering a value for that field in the adjacent text box. If you enter more than one value, separate the values with commas.			
		See "Use a WHERE clause to detect records that meet specific criteria" on page 460.			
		For example, consider an Exact Data Profile for "Employees" with a "State" field containing state abbreviations. In this example, to implement the WHERE clause, you select (check) <b>WHERE</b> , choose "State" from the drop-down list, and enter <b>CA,N</b> in the text box. This WHERE clause then limits the detection server to matching messages that contain either <b>CA</b> or <b>NV</b> as the value for the State field.			
		<b>Note:</b> You cannot specify a field for WHERE that is the same as one of the selected matched fields.			
Ignor	e Data Rows when Any	of these match			
5	Ignore data owners	Selecting this option implements Data Owner Exception.			
	(optional).	See "Configuring Data Owner Exception for EDM policy conditions" on page 398.			
6	Exclude data field combinations (optional).	You can use the exclude data field combinations to specify combinations of data values that are exempted from detection. If the data appears in exempted pairs or groups, it does not cause a match. Excluded combinations are only available when matching 2 or 3 fields. To enable this option, you must select 2 or 3 fields to match from the _ of the selected fields menu at the top of the condition configuration.			
		See "Leverage exception tuples to avoid false positives" on page 459.			
		To implement excluded combinations, select an option from each <b>Field N</b> column that appears. Then click the right-arrow icon to add the field combination to the <b>Excluded Combinations</b> list. To remove a field from the list, select it and click the left-arrow icon.			
		<b>Note:</b> Hold down the Ctrl key to select more than one field in the right-most column.			
Addit	ional match condition p	arameters			
7	Select an incident minimum.	Enter or modify the minimum number of matches required for the condition to report an incident.			
		For example, consider a scenario where you specify <b>1 of the selected fields</b> for a social security number field and an incident minimum of <b>5</b> . In this situation the engine must detect at least five matching social security numbers in a single message to trigger an incident.			
		See "Match count variant examples" on page 413.			

Steps	Action	Description
8	Select components to match on.	Select one or more message components to match on:  Envelope – The header of the message.  Subject – (Not available for EDM.)  Body – The content of the message.  Attachments – The content of any files attached to or transported by the message.  See "Selecting components to match on" on page 336.
9	Select one or more conditions to also match.	Select this option to create a compound condition. All conditions must match for the rule to trigger an incident.  You can <b>Add</b> any available condition from the list.  See "Configuring compound match conditions" on page 342.

Table 19-13 Configure the Content Matches Exact Data policy condition (continued)

### Configuring Data Owner Exception for EDM policy conditions

See "Troubleshooting policies" on page 353.

10

Test and troubleshoot

the policy.

To except data owners from detection, you must include in your Exact Data Profile either an email address or a domain address field (for example, symantec.com). Once Data Owner Exception (DOE) is enabled, if the sender or recipient of confidential information is the data owner (by email address or domain), the detection server allows the data to be sent or received without generating an incident

See "Test and tune policies to improve match accuracy" on page 361.

### To configure DOE for an EDM policy condition

- 1 When you are configuring the Content Matches Exact Data condition, select the Ignore data owners option.
- 2 Select one of the following options:
  - **Sender matches** Select this option to EXCLUDE the data sender from detection.
  - Any or All Recipient matches Select one of these options to EXCLUDE any or all data recipient(s) from detection.

Note: When you configure DOE for the EDM condition, you cannot select a value for Ignore Sender/Recipient that is the same as one of the matched fields.

See "About Data Owner Exception" on page 375.

See "About Data Owner Exception" on page 375.

### Configuring the Sender/User based on a Profiled Directory policy condition

The Sender/User based on a Directory from detection rule lets you create detection rules based on sender identity or (for endpoint incidents) user identity. This condition requires an Exact Data Profile.

See "Creating the exact data source file for profiled DGM" on page 380.

After you select the Exact Data Profile, when you configure the rule, the directory you selected and the sender identifier(s) appear at the top of the page.

Table 19-14 describes the parameters for configuring the Sender/User based on a Directory from an EDM Profile condition.

Table 19-14 Configuring the Sender/User based on a Directory from an EDM Profile condition

Parameter	Description
Where	Select this option to have the system match on the specified field values. Specify the values by selecting a field from the drop-down list and typing the values for that field in the adjacent text box. If you enter more than one value, separate the values with commas.
	For example, for an Employees directory group profile that includes a <b>Department</b> field, you would select <b>Where</b> , select <b>Department</b> from the drop-down list, and enter <b>Marketing,Sales</b> in the text box. If the condition is implemented as a rule, in this example a match occurs only if the sender or user works in Marketing or Sales (as long as the other input content meets all other detection criteria). If the condition is implemented as an exception, in this example the system ignores from matching messages from a sender or user who works in Marketing or Sales.
Is Any Of	Enter or modify the information you want to match. For example, if you want to match any sender in the Sales department, select <b>Department</b> from the drop-down list, and then enter <b>Sales</b> in this field (assuming that your data includes a Department column). Use a comma-separated list if you want to specify more than one value.

### Configuring the Recipient based on a Profiled Directory policy condition

The Recipient based on a Directory from condition lets you create detection methods based on the identity of the recipient. This method requires an Exact Data Profile.

See "Creating the exact data source file for profiled DGM" on page 380.

After you select the Exact Data Profile, when you configure the rule, the directory you selected and the recipient identifier(s) appear at the top of the page.

Table 19-15 describes the parameters for configuring Recipient based on a Directory from an EDM profile condition.

Configuring the Recipient based on a Directory from an EDM profile Table 19-15 condition

Parameter	Description
Where	Select this option to have the system match on the specified field values. Specify the values by selecting a field from the drop-down list and typing the values for that field in the adjacent text box. If you enter more than one value, separate the values with commas.
	For example, for an Employees directory group profile that includes a <b>Department</b> field, you would select <b>Where</b> , select <b>Department</b> from the drop-down list, and enter <b>Marketing</b> , <b>Sales</b> in the text box. For a detection rule, this example causes the system to capture an incident only if at least one recipient works in Marketing or Sales (as long as the input content meets all other detection criteria). For an exception, this example prevents the system from capturing an incident if at least one recipient works in Marketing or Sales.
Is Any Of	Enter or modify the information you want to match. For example, if you want to match any recipient in the Sales department, select <b>Department</b> from the drop-down list, and then enter <b>Sales</b> in this field (assuming that your data includes a Department column). Use a comma-separated list if you want to specify more than one value.

### Configuring Advanced Server Settings for EDM policies

EDM has various advanced settings available at the System > Servers > Overview > Server Detail - Advanced Server Settings screen for the chosen detection server. Use caution when modifying these settings on a server. It is recommended that you check with Symantec Data Loss Prevention Support before changing any of the settings on this screen. Changes to these settings do not take effect until after the server is restarted.

See "Advanced server settings" on page 203.

Advanced Server Settings for EDM indexing and detection Table 19-16

EDM parameter	Default	Description
EDM.MatchCountVariant	2	This setting specifies how matches are counted.  ■ 1 - Counts the number of token sets matched regardless of use of the same tokens across several matches.  ■ 2 - Counts the number of unique token sets (default).  See "Match count variant examples" on page 413.

Advanced Server Settings for EDM indexing and detection **Table 19-16** (continued)

EDM parameter	Default	Description
EDM.MaximumNumberOfMatches ToReturn	100	Defines a top limit on the number of matches returned from each RAM index search. For multi-file indices, this limit is applied to each sub-index search independently before the search results are combined. As a result the number of actual matches can exceed this limit for multiple file indices.
EDM.RunProximityLogic	true	If true (default), this setting runs the token proximity check. The free-form text proximity is defined by the setting EDM.SimpleTextProximityRadius. The tabular text proximity is defined by belonging to the same table row.  Note: Disabling proximity is not recommended because it can negatively impact the performance of the system.
EDM.SimpleTextProximityRadius	35	Provides the baseline range for proximity checking a matched token. This value is multiplied by the number of required matches to equal the complete proximity check range.  To keep the same "required match density," the proximity check range behaves like a moving window in a text page. D is defined as the proportionality factor for the window and is set in the policy condition by choosing how many fields to match on for the EDM condition. N is the SimpleTextProximityRadius value. A number of tokens are in the proximity range if the first token in is within N x D words from the last token. The proximity check range is directly proportional to the number of matches by a factor of D.  See "Proximity matching example" on page 414.  Note: Increasing the radius value higher than the default can negatively impact system performance and is not recommended.
EDM.TokenVerifierEnabled	false	Reserved for future use.
Lexer.IncludePunctuationInWords	true	If true, during detection punctuation characters are considered as part of a token.  If false, during detection punctuation within a token or multi-token is treated as white space.  See "Multi-token with punctuation" on page 406.  Note: This setting applies to detection content, not to indexed content.

Advanced Server Settings for EDM indexing and detection **Table 19-16** (continued)

EDM parameter	Default	Description	
Lexer.MaximumNumberOfTokens	12000	Maximum number of tokens extracted from each message component for detection. Applicable to all detection technologies where tokenization is required (EDM, profiled DGM, and the system patterns supported by those technologies). Increasing the default value may cause the detection server to run out of memory and restart.	
		<b>Note:</b> In Data Loss Prevention version 12.5 the default value is changed from 30,000 to 12,000. Previously, all tokens up to the limit, including stopwords and single letter words, were sent to detection. In version 12.5, the tokens sent for detection do not include stopwords or single words. The number of meaningful tokens sent to detection is approximately the same as previous versions.	
Lexer.MaxTokensPerMultiToken	10	Maximum number of sub-tokens that a multi-token cell can contain.	
		You can set this amount to as many sub-tokens as you need, but the total number of characters in a multi-token cell cannot exceed 200.	
		See "Characteristics of multi-token cells" on page 404.	
Lexer.MultiToken	true	If true cells containing spaces or punctuation are treated as multi-token cells and multi-token rules are obeyed.	
		Multi-token matching is enabled by default.	
		See "Using multi-token matching" on page 403.	
Lexer.StopwordLanguages	en	Enables the elimination of stop words for the specified languages.	
		The default is English.	
Lexer.Validate	true	If true, performs system pattern-specific validation during indexing. Setting this to false is not recommended.	
		See "Using system-provided pattern validators for EDM profiles" on page 391.	
ProfileIndex.CheckAvailableRAM	true	Specifies whether or not the amount of available RAM should be compared with a profile size before loading an EDM profile.	
ProfileIndex.MaximumInProcessIndexSize	100M	Specifies an upper limit for the maximum In Process index size. Profiles that exceed this size are loaded out of process.	
		See "Memory requirements for EDM" on page 421.	

(======================================			
EDM parameter	Default	Description	
ProfileIndex.MinimumMemoryReserve	600M	Specifies the memory reserved for out-of-process EDM algorithm execution. It is used to calculate the JVM heap size as index_size + MinumumMemoryReserve.	
		<b>Note:</b> If you see poor performance on the detection server host and CPU usage is above 60%, increase to 1000M (1 GB).	
		See "Memory requirements for EDM" on page 421.	
ProfileIndex.ProcessTimeout	60000	The time interval (in milliseconds) for launching out of process indexing. If the process is not created within this amount of time then index loading fails.	
		<b>Note:</b> In Data Loss Prevention version 12.5 the default value is changed from 10,000 to 60,000.	

Table 19-16 Advanced Server Settings for EDM indexing and detection (continued)

# Using multi-token matching

EDM policy matching is based on tokens in the index. For languages based on the Latin alphabet, a token is a word or string of alphanumeric characters delimited by spaces. For Chinese, Japanese, and Korean languages, a token is determined by other means. Tokens are normalized so that formatting and case are ignored. At run-time the server performs a full-text search against an inbound message, checking each word against the index for potential matches. The matching algorithm compares each word in the message with the contents of each token in the index.

A multi-token cell is a cell in the index that contains multiple words separated by spaces, leading or trailing punctuation, or alternative Latin and Chinese, Japanese, or Korean language characters. The sub-token parts of a multi-token cell obey the same rules as single-token cells: they are normalized according to their pattern where normalization can apply. Inbound message data must match a multi-token cell exactly, including whitespace, punctuation, and stopwords (assuming the default settings).

For example, an indexed cell containing the string "Bank of America" is a multi-token comprising 3 sub-token parts. During detection, the inbound message "bank of america" (normalized) matches the multi-token cell, but "bank america" does not.

Multi-token matching is enabled by default. Multi-token cells are more computationally expensive than single-token cells. If the index includes multi-token cells, you must verify that you have enough memory to index, load, and process the EDM profile.

See "Characteristics of multi-token cells" on page 404.

See "Memory requirements for EDM" on page 421.

### Characteristics of multi-token cells

Table 19-17 lists and describes characteristics of multi-token matching.

See "Using multi-token matching" on page 403.

Characteristics of multi-tokens Table 19-17

Characteristic	Description
Multi-token matching is configurable; by default it is enabled.	Lexer.MultiToken = true  See "Configuring Advanced Server Settings for EDM policies" on page 400.
A multi-token cell is limited to 200 total characters, including whitespace, punctuation, letters, numbers, and symbols. You cannot increase this amount, but you can configure how many sub-tokens a multi-token can contain.	Lexer.MaxTokensPerMultiToken = 10  See "Configuring Advanced Server Settings for EDM policies" on page 400.
Whitespace in multi-token cells is considered, but multiple whitespaces are normalized to 1.	See "Multi-token with spaces" on page 404.
Punctuation immediately preceding and following a token or sub-token is always ignored.	See "Multi-token with punctuation" on page 406.  See "Additional examples for multi-token cells with punctuation" on page 407.
You can configure how punctuation within a token or multi-token is treated during detection. For most cases the default setting ("true") is appropriate. If set to "false," punctuation is treated as whitespace.	Lexer.IncludePunctuationInWords = true  See "Configuring Advanced Server Settings for EDM policies" on page 400.
For proximity range checking the sub-token parts of a multi-token are counted as single tokens.	See "Proximity matching example" on page 414.
The system does not consider stopwords when matching multi-tokens. In other words, stopwords are not excluded.	See "Multi-token with stopwords" on page 405.
Multi-tokens are more computationally expensive than single tokens and require additional memory for indexing, loading, and processing.	See "Memory requirements for EDM" on page 421.

## Multi-token with spaces

Table 19-18 shows examples of multi-tokens with spaces.

Description	Indexed content	Detected content	Explanation
Cell contains space	Bank of America	Bank of America	Cell with spaces is multi-token.  Multi-token must match exactly.
Cells contains multiple spaces	Bank of America	Bank of America	Multiple spaces are normalized to one.

Table 19-18 Multi-token cell with spaces examples

### Multi-token with stopwords

Stopwords are common words, such as articles and prepositions. When creating single-tokens, the EDM indexing process ignores words found in the EDM stopword list (\SymantecDLP\Protect\config\stopwords), as well as single letters. However, when creating multi-tokens, stopwords and single letters are not ignored. Instead, they are part of the multi-token.

Table 19-19 shows multi-token matches with stopwords, single letters, and single digits.

Description	Cell content	Should match	Explanation
Cell contains stopword.	throw other ball	throw other ball	Common word ("other") is filtered out during detection but not when it is part of a multi-token.
Cell contains single letter.	throw a ball	throw a ball	Single letter ("a") is filtered out, but not when it is part of a multi-token.
Cell contains single digit.	throw 1 ball	throw 1 ball	Unlike single-letter words that are stopwords, single digits are never ignored.

Table 19-19 Cell contains stopwords or single letter or single digit

### Multi-token with mixed language characters

Table 19-20 shows examples of multi-tokens with mixed Latin and CJK characters.

Description	Cell content	Should match	Explanation
Cell includes Latin and CJK characters with no spaces.	ABC傠傫 傠傫ABC	ABC傠傫 傠傫ABC	Mixed Latin-CJK cell is multi-token.  Must match exactly.
Cell includes Latin and CJK with one or more spaces.	ABC 傠傫 傠傥 ABC	ABC 傠傫 傠傥 ABC	Multiple spaces are reduced to one.
Cell contains Latin or CJK with numbers.	什仁 仂仃 仄仅 仇仈仉 147(什仂仅 51-1)	什仁 仂仃 仄仅 仇仈仉 147(什仂仅 51-1)	Single-token cell.

Table 19-20 Multi-token cell with Latin and CJK characters examples

### Multi-token with punctuation

Punctuation is always ignored if it comes at the beginning (leading) or end (trailing) of a token or multi-token. Whether punctuation included in a token or multi-token is required for matching depends on the Advanced Server Setting

Lexer.IncludePunctuationInWords, which by default is set to true (enabled).

See "Multi-token punctuation characters" on page 412.

Note: For convenience purposes the Lexer. Include Punctuation In Words parameter is referred to by the three-letter acronym "WIP" throughout this section.

The WIP setting operates at detection-time to alter how matches are reported. For most EDM policies you should not change the WIP setting. For a few limited situations, such as account numbers or addresses, you may need to set IncludePunctuationInWords = false depending on your detection requirements.

See "Multi-token punctuation characters" on page 412.

Table 19-21 lists and explains how multi-token matching works with punctuation.

Table 19-21 Multi-token punctuation table

Indexed content	Detected content	WIP setting	Match	Explanation
a.b	a.b	TRUE	Yes	The indexed content and the detected content are exactly the same.
		FALSE	No	The detected content is treated as "a b" and is therefore not a match.

Indexed content	Detected content	WIP setting	Match	Explanation
a.b	a b	TRUE	No	The indexed content and the detected content are different.
		FALSE	No	The indexed content and the detected content are different.
a b	a.b	TRUE	No	The indexed content and the detected content are different.
		FALSE	Yes	The detected content is treated as "a b" and is therefore a match.
a b	a b	TRUE	Yes	The indexed content and the detected content are exactly the same
		FALSE	Yes	The indexed content and the detected content are exactly the same

Table 19-21 Multi-token punctuation table (continued)

### Additional examples for multi-token cells with punctuation

Table 19-22 lists and describes some additional examples for multi-token cells with punctuation. In these examples, the main thing to keep in mind is that during indexing, if a token includes punctuation marks between characters the punctuation is always retained. This means that EDM cannot detect that cell if the WIP setting is false. In other words, if indexed data has cell which has a token with internal punctuation, the WIP setting should be set to true.

Table 19-22 Additional use cases for multi-token cells with punctuation

Description	Indexed content	Detected content	Explanation
Cell contains a physical address with punctuation.	346 Guerrero St., Apt. #2	346 Guerrero St., Apt. #2 346 Guerrero St Apt 2	The indexed content is a multi-token cell.  Both match because the punctuation comes at the beginning or end of the sub-token parts and is therefore ignored.

Additional use cases for multi-token cells with punctuation **Table 19-22** (continued)

Description	Indexed content	Detected content	Explanation
Cell contains internal punctuation with no space	O'NEAL ST.	O'NEAL ST	The indexed content is a multi-token cell.
before or after.			Internal punctuation is included (assuming WIP is true), and leading or trailing punctuation is ignored (assuming there is a space delimiter after the punctuation).
Cell contains Asian language characters (CJK)	傠傫;;傠傫	傠傫;;傠傫 (if WIP true)	The indexed content is a single token cell.
with indexed internal punctuation.			During detection, Asian language characters (CJK) with internal punctuation is affected by the WIP setting. Thus, in this example 傠课;; 傠课 matches only if the WIP setting is true.
			If the WIP setting is false, 傠 像;;傠像 is considered a multi-token because the internal punctuation is treated as whitespace. Thus, no content can match.
Cell contains Asian language characters (CJK)	傠傫 傠傫	信像信像	The indexed content is a multi-token cell.
without indexed internal punctuation.		傠傫;;傠傫 (if WIP false)	The detected content matches as indexed. If the WIP setting is false, the detected content matches 傠傫;;傠傫 because internal punctuation is ignored.

Additional use cases for multi-token cells with punctuation **Table 19-22** (continued)

Description	Indexed content	Detected content	Explanation
Cell contains mix of Latin and CJK characters with	EDM;;傠傫	EDM 傠傫	The indexed content is a multi-token cell.
punctuation separating the Latin and Asian characters.			A cell with alternate Latin and CJK characters is always a multi-token and punctuation between Latin and Asian characters is always treated as a single white space regardless of the WIP setting.
Cell contains mix of Latin and CJK characters with	DLP;;EDM 傠傫;;傠傥	DLP;;EDM;;傠傫;;傠傥 (if WIP true)	The indexed content is a multi-token cell.
internal punctuation.		DLP;;EDM 傠傫;;傠傥 (if WIP true)	During detection, punctuation between the Latin and Asian characters is treated as a single whitespace and leading and trailing punctuation is ignored.
			If the WIP setting is true the punctuation internal to the Latin characters and internal to the Asian character is retained.
			If the WIP setting is false, no content can match because internal punctuation is ignored.

Description Indexed content **Detected content Explanation** Cell contains mix of Latin DLP EDM 傠傫 傠傥 DLP EDM 傠傫 傠傥 The indexed content is a and CJK characters with multi-token cell. DLP;EDM 傠傫;傠傥 (if WIP internal punctuation. false) During detection. punctuation between the DLP;EDM;; 傠傫; 傠傥 (if WIP Latin and Asian characters false) is treated as a single whitespace and leading and trailing punctuation is ignored. Thus, it matches as indexed. If the WIP setting is false, it matches DLP;EDM;; 傠傫; 傠 傥 because internal punctuation is ignored.

Table 19-22 Additional use cases for multi-token cells with punctuation (continued)

### Some special use cases for system-recognized data patterns

EDM provides validation for and recognition of the following special data patterns:

- Credit card number
- Email address
- IP address
- Number
- Percent
- Phone number (US, Canada)
- Postal code (US, Canada)
- Social security number (US SSN)

See "Using system-provided pattern validators for EDM profiles" on page 391.

Note: It is a best practice to always validate your index against the recognized system patterns when the data source includes one or more such column fields. See "Map data source column to system fields to leverage validation" on page 455.

The general rule for system-recognized patterns is that the WIP setting does not apply during detection. Instead, the rules for that particular pattern apply. In other words, if the pattern is recognized during detection, the WIP setting is not checked. This is always true if the pattern is a string of characters such as an email address, and if the cell contains a number that conforms to one of the recognized number patterns (such as CCN or SSN).

In addition, even if the pattern is a generic number such as account number that does not conform to one of the recognized number patterns, the WIP setting may still not apply. To ensure accurate matching for generic numbers that do not conform to one of the system-recognized patterns, you should not include punctuation in these number cells. If the cell contents conforms to one of the system-recognized patterns, the punctuation rules for that pattern apply and the WIP setting does not.

See "Do not use the comma delimiter if the data source has number fields" on page 455.

See Table 19-23 on page 411. lists and describes examples for detecting system-recognized data patterns.

Caution: This list is not exhaustive. It is provided for informational purposes only to ensure that you are aware that data that matches system-defined patterns takes precedence and the WIP setting is ignored. Before deploying your EDM policies into production, you must test detection accuracy and adjust the index accordingly to ensure that the data that you have indexed matches as expected during detection.

Table 19-23 Some special use cases for system-recognized data patterns

Description	Indexed content	Detected content	Explanation
Cell contains an email address.	person@example.com	person@example.com	An email address is indexed and detected as a single-token regardless of the WIP setting. It must match exactly as indexed. If you were to set WIP to false, "person example com" would not match as a multi-token and does not match the indexed single-token.

	(continued)				
Description	Indexed content	Detected content	Explanation		
Cells contains a 10-digit account number.	#########	######################################	The WIP setting is ignored because the number conforms to the phone number pattern and its rules take precedence.		
	## ###### ##	## ###### ##	Must match exactly. The pattern ## ####### does not match even if WIP is set to false.		
	### #### ###	### #### ###	Must match exactly. The pattern ###-#### does not match even if WIP is set to false.		

**Table 19-23** Some special use cases for system-recognized data patterns (continued)

### Multi-token punctuation characters

In EDM, a multi-token cell is any cell that has been indexed that contains punctuation (as well as spaces or alternative Latin words and CJK characters).

See Table 19-24 on page 412.

Using multi-token matching lists the symbols that are identified and treated as punctuation during EDM indexing.

**Table 19-24** Characters treated as punctuation for indexing

Punctuation name	Character representation
Apostrophe	•
Tilde	~
Exclamation point	!
Ampersand	&
Dash	-
Single quotation mark	•
Double quotation mark	
Period (dot)	

**Table 19-24** Characters treated as punctuation for indexing (continued)

Punctuation name	Character representation
Question mark	?
At sign	@
Dollar sign	\$
Percent sign	%
Asterisk	*
Caret symbol	Λ
Open parenthesis	(
Close parenthesis	)
Open bracket	]
Close bracket	]
Open brace	{
Close brace	}
Right arrow	>
Left arrow	<
Forward slash	1
Back slash	1
Pound sign	#
Equal sign	=
Plus sign	+
Semicolon	;

## Match count variant examples

The default value for the Advanced Server setting EDM.MatchCountVariant eliminates matches that consists of the same set of tokens from some other match. Rarely is there a need to change the default value, but if necessary you can configure how EDM matches are counted using this parameter.

See "Advanced server settings" on page 203.

Table 19-25 provides examples for match counting. All examples assume that the policy is set to match 3 of 4 column fields and that the profile index contains the following cell contents:

Kathy | Stevens | 123-45-6789 | 1111-1111-1111

Kathy | Stevens | 123-45-6789 | 2222-2222-2222

Kathy | Stevens | 123-45-6789 | 3333-3333-3333-3333

Table 19-25 Match count variant examples

Inbound message contents	Match count variant	Number of matches	Explanation
Kathy Stevens 123-45-6789	1	3	Records matched in the profile: first name, last name, SSN.
	2 (default)	1	Number of unique token sets matched.
Kathy Stevens 123-45-6789 1111-1111-1111	1	3	Records matched in the profile (up to the required number of matches [3]).
Kathy Stevens 123-45-6789	2	1	EDM matches the left-most tokens for each profile data row. Thus, the token set for each row is as follows:
			Row # 1: Kathy Stevens 123-45-6789
			Row # 2: Kathy Stevens 123-45-6789
			Row # 3: Kathy Stevens 123-45-6789
1111-1111-1111 Kathy	2	2	The token set for each row is as follows:
Stevens 123-45-6789			Row # 1: 1111-1111-1111 Kathy Stevens
			Row # 2: Kathy Stevens 123-45-6789
			Row # 3: Kathy Stevens 123-45-6789

## Proximity matching example

EDM protects confidential data by correlating uniquely identifiable information, such as SSN, with data that is not unique, such as last name. When correlating data, it is important to ensure that terms are related. In natural languages, it is more likely that when two words appear close together they are being used in the same context and are therefore related.

Based on the premise that word proximity indicates relatedness, EDM employs a proximity-matching radius or range to limit how much freeform content the system will examine when searching for matches. EDM proximity matching is designed to reduce false positives by ensuring that matched terms are proximate.

The proximity range is proportional to the policy definition. The proximity range is determined by the proximity radius multiplied by the number of matches required by the EDM policy condition. The radius is set by the Advanced Server Setting parameter EDM. SimpleTextProximityRadius. The default value is 35. In addition, proximity matching applies to both free-form text and tabular data. There is no distinction at run-time between the two. Thus, tabular data is treated the same as free text data and the proximity check is performed beyond the scope of the length of the row contents

For example, assuming the default radius of 35 and a policy set to match 3 out of 4 column fields, the proximity range is 105 tokens (3 x 35). If the policy matches 2 out of 3 the proximity range is 70 tokens (35 x 2).

Warning: While you can decrease the value of the proximity radius, Symantec does not recomment increasing this value beyond the default (35). Doing so may cause performance issues. See "Configuring Advanced Server Settings for EDM policies" on page 400.

Table 19-26 shows a proximity matching example based on the default proximity radius setting. In this example, the detected content produces 1 unique token set match, described as follows:

- The proximity range window is 105 tokens (35 x 3).
- The proximity range window starts at the leftmost match ("Stevens") and ends at the rightmost match ("123-45-6789").
- The total number of tokens from "Stevens" to the SSN (including both) is 105 tokens.
- The stopwords "other" and "a" are counted for proximity range purposes.
- "Bank of America" is a multi-token. Each sub-token part of a multi-token is counted as a single token for proximity purposes.

Indexed data	Policy	Proximity	Detected content
Last_Name   Employer   SSN Stevens   Bank of America   123-45-6789	Match 3 of 3	Radius = 35 tokens (default)	Zendrerit inceptos Kathy <b>Stevens</b> lorem ipsum pharetra convallis leo suscipit ipsum sodales rhoncus, vitae dui nisi volutpat augue maecenas in, luctus id risus magna arcu maecenas leo quisque. Rutrum convallis tortor urna morbi elementum hac curabitur morbi, nunc dictum primis elit senectus faucibus convallis surfrent. Aptentnour gravida adipiscing iaculis himenaeos, himenaeos a porta etiam viverra. Class torquent uni other tristique cubilia in <b>Bank of America</b> . Dictumst lorem eget ipsum. Hendrerit inceptos other sagittis quisque. Leo mollis per nisl per felis, nullam cras mattis augue turpis integer pharetra convallis suscipit hendrerit? Lubilia en mictumst horem eget ipsum. Inceptos urna sagittis quisque dictum odio hendrerit convallis suscipit ipsum wrdsrf <b>123-45-6789</b> .

**Table 19-26** Proximity example

## **Updating EDM indexes to version 12.5**

If you are upgrading to Symantec Data Loss Prevention 12.5 and want to take advantage of new features, including multi-token cell matching and proportional proximity matching, you must update each Exact Data profile by reindexing the data source using the 12.5 EDM Indexer. While legacy EDM indexes will run on 12.5 detection servers, you will not be able to use a legacy EDM index with the new features. In addition, you need to verify the amount of memory required for indexing the data source, and loading and processing the index at run-time on the detection server.

See "About upgrading EDM deployments" on page 377.

See "Memory requirements for EDM" on page 421.

If you do not reindex the data source file, the system presents error messages indicating that the Exact Data profile is out of date and must be reindexed, and that you need to calculate memory requirements.

See "EDM index out of date error codes" on page 420.

There are two primary 12.5 upgrade scenarios for EDM:

 You use the Remote EDM Indexer to create 12.5-compliant indexes remotely and copy them to the Enforce Server.

See "Update process using the Remote EDM Indexer" on page 417.

 You already have a data source file that is current and cleansed that you can copy to the upgraded 12.5 Enforce Server for indexing. See "Update process using the Enforce Server" on page 419.

### Update process using the Remote EDM Indexer

Consider the following procedure for upgrading your EDM deployments to Symantec Data Loss Prevention 12.5. This procedure assumes that you can remotely index the data source and copy the index file to the Enforce Server.

See "Remote EDM indexing" on page 432.

If remote indexing is not possible, the other option for upgrade is to copy the data source file to the 12.5 Enforce Server.

See "Update process using the Enforce Server" on page 419.

Table 19-27 Update process using the Remote EDM Indexer

Step	Action	Description
1	Upgrade the Enforce Server to 12.5.	Refer to the <i>Symantec Data Loss Prevention 12.5 Upgrade Guide</i> for details. Do not upgrade the EDM detection server(s) at this point.  The 12.5 Enforce Server can continue to receive incidents from non-12.5 detection servers during the upgrade process. Policies and other data cannot be pushed out to non-12.5 detection servers (one-way communication only between Enforce 12.5 and non-12.5 detection servers).
2	Create a 12.5-compatible remote EDM profile template.	Using the 12.5 Enforce Server administration console, create a new EDM profile template for remote EDM indexing.  See "Creating an EDM profile template for remote indexing" on page 436.  Download the *.edm profile template and copy it to the remote data source host system.  See "Downloading and copying the EDM profile file to a remote system" on page 439.
3	Install the 12.5 Remote EDM Indexer on the remote data source host.	Install the Symantec Data Loss Prevention 12.5 Remote EDM Indexer on the remote data source host and index the data source.  See "Remote EDM indexing" on page 432.
4	Calculate the memory required to index the data source and adjust the indexer memory setting.	Calculate the memory required for indexing before you attempt to index the data source. Although the Remote EDM Indexer is allocated sufficient memory to index most data sources, if you have a very large index you may have to allocate more memory.  See "Memory requirements for EDM" on page 421.

#### Update process using the Remote EDM Indexer (continued) **Table 19-27**

Step	Action	Description
4	Index the data source using the 12.5 Remote EDM	The result of this process is 1 or more *.rdx files that are 12.5 compatible that you can load into a 12.5 Enforce Server system.
	Indexer.	If you have a data source file prepared, run the Remote EDM Indexer and index it.
		See "Remote indexing examples using data source file" on page 440.
		If the data source is an Oracle database and the data is clean, use the SQL Preindexer to pipe the data to the Remote EDM Indexer.
		See "Remote indexing examples using SQL Preindexer" on page 441.
5	Calculate the memory required to load and process the index and adjust the	You need to calculate how much RAM the detection server requires to load and process the index and run-time. These calculations are required for each EDM index you want to deploy and the memory adjustments are cumulative.
detection server memory setting for each EDM detection server host.		See "Memory requirements for EDM" on page 421.
6	Update the EDM profile by loading the 12.5 index	Copy the *.pdx and one or more *.rdx files from the remote host to the 12.5 Enforce Server host file system.
		Load the index into the EDM profile you created in Step 2.
		See "Copying and loading remote index files to the Enforce Server" on page 442.
7	Upgrade one or more EDM detection server to 12.5.	Once you have created the 12.5 compliant EDM proflies and upgraded the Enforce Server, you can then upgrade the detection server(s).
		Refer to the Symantec Data Loss Prevention 12.5 Upgrade Guide for details.
		Make sure you have calculated and verified the memory requirements for loading and processing multi-token indexes on the detection server.
		See "Memory requirements for EDM" on page 421.
8	Test and verify the updated index.	Legacy EDM indexes and policies will run on 12.5 detection servers but will not make use of 12.5 features. To test the upgraded system and updated index, you can create a new policy that references the updated index. Meanwhile, the legacy index and policy remains deployed and running.
9	Remove out-of-date EDM indexes.	Once you have verified the new EDM index and policy, you can retire the legacy EDM index and policy.

## Update process using the Enforce Server

Consider the following index update procedure if remote indexing is not possible and you have a current data source file that you can copy to the Enforce Server.

Update process using the Enforce Server Table 19-28

Step	Action	Description	
этер	Action	Description	
1	Upgrade the Enforce Server to 12.5.	Refer to the Symantec Data Loss Prevention 12.5 Upgrade Guide for details.	
	10 12.5.	Do not upgrade the EDM detection server(s) at this point.	
		The 12.5 Enforce Server can continue to receive incidents from non-12.5 detection servers during the upgrade process. Policies and other data cannot be pushed out to non-12.5 detection servers (one-way communication only between Enforce 12.5 and non-12.5 detection servers).	
2	Create, prepare, and copy the data source file to the	Copy the data source file to the /SymantecDLP/Protect/datafiles directory on the upgraded 12.5 Enforce Server host file system.	
	12.5 Enforce Server host.	See "Creating the exact data source file for EDM" on page 379.	
		See "Preparing the exact data source file for indexing" on page 381.	
		See "Uploading exact data source files to the Enforce Server" on page 383.	
3	Calculate memory the memory required to index	Calculate the memory required for indexing before you attempt to index the data source.	
	the data source and update the indexer memory setting.	See "Memory requirements for EDM" on page 421.	
4 Create a new 12.5 compliant EDM profile and		Create a new EDM profile using the 12.5 Enforce Server administration console.	
	index the data source file.	Choose the option <b>Reference Data Source on Manager Host</b> for uploading the data source file (assuming you copied it to the /datafiles directory).	
		Index the data source file on save of the profile.	
		See "Creating and modifying Exact Data Profiles" on page 385.	
5	Calculate memory the memory required to load and process the index at run-time and adjust the	You need to calculate how much RAM the detection server requires to load and process the index and run-time. These calculations are required for each EDM index you want to deploy and the memory adjustments are cumulative.	
	memory settings for each EDM detection server host.	See "Memory requirements for EDM" on page 421.	

Step	Action	Description	
6	Upgrade the EDM detection server(s) to 12.5.	Once you have created the 12.5-compliant EDM profile you can then upgrade the detection server(s).	
		Refer to the Symantec Data Loss Prevention 12.5 Upgrade Guide for details.	
		Make sure you have calculated and verified the memory requirements for loading and processing multi-token indexes on the detection server.	
		See "Memory requirements for EDM" on page 421.	
7	Test and verify the updated index.	Legacy EDM indexes and policies will run on 12.5 detection servers but will not make use of 12.5 features. To test the upgraded system and updated index, you can create a new policy that references the updated index. Meanwhile, the legacy index and policy remains deployed and running.	
8	Remove out-of-date EDM indexes.	Once you have verified the new EDM index and policy, you can retire the legacy EDM index and policy.	
		See "Remote EDM indexing" on page 432.	

Table 19-28 Update process using the Enforce Server (continued)

### EDM index out of date error codes

Symantec Data Loss Prevention version 12.5 provides several enhancements for EDM. To take advantage of these enhancements, you must reindex the data source for each Exact Data profile using the 12.5 EDM Indexer. Although legacy EDM indexes will run on 12.5 detection servers, such indexes do support 12.5 features.

If your EDM index is not 12.5-compliant, the system informs you with error messages. Table 19-29 lists the error codes that the system displays if the EDM index is out of date and not compatible with the current Symantec Data Loss Prevention version.

Table 19-29 Error messages for non-complia	iant Exa	act Data Profiles	,
--	----------	-------------------	---

Error message type	Error code	Error message
Enforce Server error event	2928	One or more profiles are out of date and must be reindexed. Please refer to the "Memory requirements for EDM" section in the Symantec DLP Administration Guide for additional information.
		See "Updating EDM indexes to version 12.5" on page 416.
		See "Memory requirements for EDM" on page 421.
Enforce Server error event detail	2928	Check the <b>Manage &gt; Data Profiles &gt; Exact Data</b> page for more details. The following EDM profiles are out of date: Profile X, Profile XY, and so forth.

Error message type	Error code	Error message
System Event error	2928	One or more profiles are out of date and must be reindexed.
Exact Data Profile error	N/A	This profile is out of date, and must be reindexed.

Table 19-29 Error messages for non-compliant Exact Data Profiles (continued)

# Memory requirements for EDM

Symantec Data Loss Prevention version 12.5 supports multi-token matching. Multi-token matching is enabled by default.

See "Using multi-token matching" on page 403.

A multi-token is more computationally expensive than a single-token. If you are using multi-token matching, you need to verify that the amount of memory allocated to the indexer and to the detection server(s) is sufficient for each EDM index. You may need to increase the memory allocated to the indexer and for the detection server(s).

Memory requirements cannot be generalized because each index is unique. Determining the memory requirements for a multi-token index is a three-step process in which you calculate the memory required for indexing, loading, and processing.

Note: You must perform the memory calculations if you are using multi-token matching. This means that your index contains multi-token cells and multi-token matching is enabled. If your index does not contain multi-token cells, or you have disabled multi-token matching, you only need to perform Step 2 of the memory calculations.

Table 19-30 describes the process for calculating and adjusting the memory requirements for the indexer and the detection server(s) when you are using multi-token matching.

 $Work flow for determining memory \, requirements \, for \, EDM \, multi-token \,$ **Table 19-30** indexes

Step	Action	Description
1	Determine the memory required to index the data source.	This calculation is based on the number of multi-token cells in the index and the memory requirements for multi-tokens.
		See "Determining how much memory is needed to index the data source" on page 424.
		See "Multi-token memory table" on page 423.
		You ADD the result of this calculation to the existing RAM allocated to the indexer. Restart the Vontu Manager service after updating the memory setting.
		See "Increasing the memory for the Enforce Server EDM indexer" on page 429.
		<b>Note:</b> If you are using the Remote EDM indexer, you do not have to allocate more RAM for indexing unless the index has an extremely large number of multi-token cells. See "Increasing the memory for the Remote EDM indexer" on page 429.
2	Determine the memory required to load the index into memory on the detection server.	This calculation is roughly 2 GB x the number of *.rdx files comprising the index, if 2 or more. If the index comprises 1 *.rdx file, the file size on disc is the factor.
		You use the result of this calculation establish the minimum amount of memory needed to load the index into RAM on the detection server host.
		See "Determining how much memory is needed to load the index into memory on the detection server" on page 426.
		<b>Note:</b> This step is required even if the index is not a multi-token index.

Table 19-30 Workflow for determining memory requirements for EDM multi-token indexes (continued)

Step	Action	Description
3	Determine additional memory required to process the index during detection.	To get this calculation you double the result of the first calculation you made in Step 1 and add this sum to the memory load calculation. Update the File Reader memory setting with the result and restart the detection server.
		See "Determining and setting the memory for the detection server" on page 427.
		See "Increasing the memory for the detection server (File Reader)" on page 430.
		<b>Note:</b> The detection server memory requirements are cumulative for each EDM index. In other words, for each index you determine the amount of memory required to load and process it, and ADD this amount to the existing amount of RAM that is allocated to that server.
4	Repeat for each EDM index you want to deploy.	The three-step calculation process is required for each multi-token index you plan to deploy. Keep in mind that you only adjust the detection server memory settings for the server where the index will be loaded and processed at run-time.
		See "Additional example memory requirement calculations" on page 431.

### Multi-token memory table

Table 19-31 lists and describes the amount of additional memory (in bytes) that are required for multi-token indexes. You use these numbers to calculate memory requirements for EDM indexing and processing.

Note that the first 16 million multi-token cells require 32 bytes per cell while additional multi-token cells require 8 bytes per cell. Note also that the memory requirements for loading and processing are double the requirements for indexing.

**Table 19-31** EDM multi-token memory requirements

Number of multi-token cells	Indexer memory requirements	Detection server memory requirements to load and process the index
Up to 16 million	32 bytes per multi-token cell	64 bytes per multi-token cell
Above 16 million	8 bytes per multi-token cell	16 bytes per multi-token cell

### EDM index size table

Table 19-32 provides the default size thresholds for small, medium, and large indexes. If you have a small or medium size index, the index comprises a single \*.rdx file. If you have a large EDM index, the index spans multiple \*.rdx files.

EDM index sizes **Table 19-32** 

Size of index on disk	Identifier	# of RDX files	Description
100 MB or less	Small	1	<pre>Indexing is performed in process. ProfileIndex.MaximumInProcessIndexSize = 100 MB (default)</pre>
More than 100 MB	Medium	1	<pre>Indexing is performed out of process. ProfileIndex.MaximumInProcessIndexSize = 100 MB (default)</pre>
1.3 GB or more	Large	2 or more	Index spans multiple *.rdx files.  max_loaded_index_memory = 1378 MB (default)

### Determining how much memory is needed to index the data source

Table 19-33 provides the steps for determining how much memory is needed to index the data source.

**Table 19-33** Determine memory requirements for indexing

Step	Action	Description
1	Estimate the number of multi-tokens in the index.	Multiply the total number of rows or records in the data source by the number of multi-token columns.
		For example, if your index has 100 million rows and 3 of the 5 columns in the index contain multi-token values, the estimated number of multi-token cells is 300 million.

Determine memory requirements for indexing (continued) **Table 19-33** 

Step	Action	Description
2	Perform the calculation.	Refer to the memory table to perform the following calculation.
		See Table 19-31 on page 423.
		First you determine the amount of additional memory needed for the first 16 million multi-tokens.
		For example, if your index has an estimated 300 million multi-token cells, the additional memory required to index the first 16 million rows in the data source is calculated as follows
		16 million multi-token cells * 32 bytes = 512 million bytes of additional memory
		Next you determine the additional memory required for the remaining multi-token cells. For example:
		284 million multi-token cells * 8 bytes = 2.272 million bytes of additional memory
		Finally, to get the total additional RAM required to index the data source you add the results:
		512 million bytes + 2.272 million bytes = 2.784 million bytes = 2.6 GB (rounded)
3	Increase the indexer memory.	The next step is to increase the memory allocated to the indexer. The procedure for increasing the indexer memory differs depending on whether you are using the EDM indexer local to the Enforce Server or the Remote EDM Indexer.
		<b>Note:</b> Whichever indexer you use, make sure you ADD the calculation to the existing or default memory allocation and that you do not replace the existing or default setting with the calculation.
		See "Increasing the memory for the Enforce Server EDM indexer" on page 429.
		See "Increasing the memory for the Remote EDM indexer" on page 429.
4	Restart the Vontu Manager service.	You must restart this service after you have changed the memory allocation.
5	Index the data source.	The last step is to index the data source. You need to do this before you calculate remaining memory requirements.
		See "Creating and modifying Exact Data Profiles" on page 385.

### Determining how much memory is needed to load the index into memory on the detection server

The next step in the workflow is to determine the amount of memory required to load the index into memory on the detection server. This calculation depends on the size of the index on disc.

Table 19-34 provides the steps for performing the calculation to determine the baseline memory that you must allocate to the detection server to load the index into RAM.

Table 19-34 Determine memory requirements for indexing

Step	Action	Description
1	Count the number of indexes deployed to a detection server.	If you have a small or medium size index, you will have only one $*.rdx$ file.
		If you have a large index, you will have multiple *.rdx files.
		See "Multi-token memory table" on page 423.

Table 19-34 Determine memory requirements for indexing (continued)

Step	Action	Description
2	Perform the calculation.	If the index comprises only 1 file (small or medium index), get the size of the index on disc. For example, if the size of the index on disc is 500MB, this is the baseline amount of memory you need to load the index. You then proceed to the next step to determine additional memory to process the index.
		See "Determining and setting the memory for the detection server" on page 427.
		If the index is large and comprises multiple *.rdx files, you add the number of *.rdx files comprising the index and multiply that number by 1.9 GB.
		For example, if the index comprises $3 *.rdx$ files, the calculation is $3 * 1.9 = 5.7$ GB. This is the baseline amount of memory you need to load the index into RAM on the detection server.
		The 1.9 GB factor is derived from the following two settings and their default values:
		<pre>Indexer.properties:max_loaded_index_memory = 1378M (1.3 GB rounded)</pre>
		Advanced Server Setting: ProfileIndex.MinimumMemoryReserve 600M (600 MB)
		If you have changed either of these settings you will need to adjust the factor accordingly. For example, if for performance reasons you change the value of the ProfileIndex.MinimumMemoryReserve parameter from 600M to 1000M (1 GB), the factor is 2.3 GB.
		See "Configuring Advanced Server Settings for EDM policies" on page 400.
3	Perform another calculation to determine additional memory.	See "Determining and setting the memory for the detection server" on page 427.

### Determining and setting the memory for the detection server

The last step in the workflow is to determine the amount of memory required to process the index at run-time. The easiest way to perform this calculation is simply to double the calculation you performed to determine how much memory is required to index the data source. You add the result to the amount of memory required to load the index. You then use this figure to adjust the memory for the File Reader on the detection server.

Table 19-35 describes the process for calculating the additional memory required on the detection server to process the index.

Determine memory requirements for indexing **Table 19-35** 

Step	Action	Description
1	Count the number of multi-token cells in the index.	Multiply the total number of rows or records in the data source by the number of multi-token columns.
		For example, if your index has 100 million rows and 3 of the 5 columns in the index contain multi-token values, the estimated number of multi-token cells is 300 million.
2	Perform the calculation.	Use the memory table to perform the calculation.
		See Table 19-31 on page 423.
		For example, if your index has an estimated 300 million multi-token cells, the additional memory required to index the data source is calculated as follows:
		16 million multi-token cells * 64 bytes = 1.024 million bytes of additional memory
		Next you determine the additional memory required for the remaining multi-token cells.
		284 million multi-token cells * 16 bytes = 4.544 million bytes of additional memory
		To get the total additional RAM required to index the data source you add the results:
		1.024 million bytes + 4.544 million bytes = 5.568 million bytes = 5.2 GB (rounded)
3	Add the amounts.	Add the amount you calculated above to the amount you calculated for the initial loading of the index.
		See "Determining how much memory is needed to load the index into memory on the detection server" on page 426.
		For example, if the index comprises 3 * .rdx files:
		1.9 GB * 3 = 5.7 GB + 5.2 GB = 10.9 GB required to load the index and run the index on the detection server.
		Or, if the index comprises 1 *.rdx file with a size of 100 MB:
		100 MB + 5.2 GB = 5.3 GB required to load and process the index at run-time.
4	Increase the File Reader memory.	See "Increasing the memory for the detection server (File Reader)" on page 430.

### Increasing the memory for the Enforce Server EDM indexer

Complete the following steps to increase the memory for the Enforce Server indexer.

These steps assume you have performed the indexer calculations.

### To increase the memory for the Enforce Server indexer

- 1 Open the file \SymantecDLP\protect\config\VontuManager.conf
- 2 Locate the following "Initial Java Heap Size (in MB)" parameter wrapper.java.maxmemory = 2048 (the default value is 2048 MB (2 GB); your value may be different if you changed it)
- 3 ADD the value of your calculation to the maxmemory setting.

For example, if by your calculation you determine that you need an additional 2.6 GB of RAM, you would increase the value by an additional 2662 MB

Note: This result is ADDED to the existing memory setting; it is not used to replace the existing memory setting.

wrapper.java.maxmemory = 4710 (the default value 2048 plus the additional calculation of 2662)

- 4 Save the VontuManager.conf file.
- Restart the Vontu Manager service.

### Increasing the memory for the Remote EDM indexer

The Remote EDM Indexer runs with the default JMV settings. This means that the Remote EDM Indexer is allocated approximately 25% of the to total RAM that the computer has installed. (Consult the JVM documentation for precise details.)

For most data sources, the default memory settings are sufficient for remote indexing. However, if you have a very large multi-token index, you may need to increase the amount of RAM allocated to the Remote EDM Indexer. In Symantec Data Loss Prevention testing, multi-token indexes over 20 GB in size required additional memory allocated for the Remote EDM Indexer. However, smaller indexes may require additional memory for remote indexing depending on the nature of the index or the size of the host hardware.

You set the JVM heap size for the Remote EDM Indexer process by creating a \*.vmoptions file and deploying it to the Remote EDM Indexer host.

The \*.vmoptions file accepts one JVM option per line. For example, you can specify the following options in a file you save as RemoteEDMIndexer.vmoptions:

-Xms1378M

-Xmx11G

In this example, the initial memory allocation size (-xms1378M) is the same amount that is allocated to the indexer that is local to the Enforce Server. See the wrapper.java.initmemory parameter in the VontuManager.conf file. The maximum size (-Xmx11g) is based on your multi-token calculations.

See "Determining how much memory is needed to index the data source" on page 424.

To deploy the \*.vmotpions file, copy it to the following locations:

For Linux: /opt/SymantecDLP/Protect/bin/RemoteEDMIndexer.vmoptions

For Windows: \SymantecDLP\Protect\bin\RemoteEDMIndexer.exe.vmoptions

See "Generating remote index files" on page 439.

### Increasing the memory for the detection server (File Reader)

This topic provides instructions for increasing the File Reader memory allocation for a detection server.

These instructions assume you have performed the necessary calculations.

See "Determining how much memory is needed to load the index into memory on the detection server" on page 426.

See "Determining and setting the memory for the detection server" on page 427.

### To increase the memory for detection server processing

- In the Enforce Server administration console, navigate to the Server Detail -Advanced Server Settings screen for the detection server where the EDM index is deployed or to be deployed.
- Locate the following setting: BoxMonitor.FileReaderMemory. 2
- Change the -Xmx4G value in the following string to match the calculations you have made.
  - -Xrs -Xms1200M -Xmx4G -XX:PermSize=128M -XX:MaxPermSize=256M

For example: -Xrs -Xms1200M -Xmx11G -XX:PermSize=128M

-XX:MaxPermSize=256M

Save the configuration and recycle the detection server.

### Additional example memory requirement calculations

This section provies additional examples of EDM memory calculations for multi-token and single-token indexes. If you have enough memory to forgo precise calculations or need a quick estimate, you can perform these short-cut example calculations.

Table 19-36 provides an example calculation if the index contains multi-token cells and it comprises 2 or more \*.rdx files. In this case you multiply the number of \*.rdx files by 2 GB to get the amount of memory required to load the index.

Example memory calculation for a multi-token index comprising **Table 19-36** multiple \*.rdx files

Step	Action	Example
1	Perform the indexing calculation as described and index the data source.	If the data source has approximately 300 million multi-token cells:
	See "Determining how much memory is needed to index the data source" on page 424.	16 million * 32 bytes + 284 million * 8 bytes = 2.6 GB required to index the data source
		You then add 2.6 GB to the existing amount of RAM allocated to the indexer process.
2	Perform the load calculation by multiplying the number of *.rdx files by 2 GB (rounding up 1.9 to 2).	If the index comprises 3 files, then:  3 * . rdx files * 2 GB each = 6 GB required to load the index on the detection server
3	Perform the run-time processing calculation by doubling the result of the index calculation (Step 1) and adding it to the result of the load calculation (Step 2).	2.6 GB * 2 = 5.2 GB + 6 GB = 11.2 GB  This is the total memory required for the detection server to load and process THIS index.

Table 19-37 provides an example calculation if the index only comprises 1 \*.rdx file. In this case you use the size of the file on disk to get the amount of memory required to load the index.

Example memory calculation for a multi-token index comprising a Table 19-37 single \* . rdx file

Step	Action	Example
1	Perform the indexing calculation as described and index the data source.	Multiply the first 16 million multi-token cells in the index by 32 bytes.
	See "Determining how much memory is needed to index the data source" on page 424.	Multiple the remaining multi-token cells in the index by 8 bytes.
		Add the results.

		. ,
Step	Action	Example
2	Perform the load calculation by checking the size of the *.rdx file on disk.	If the size of the $*.rdx$ file on disk is 500 MB, then this is the amount of RAM required by the detection server to load the index.
3	Perform the run-time processing calculation by doubling the result of the index calculation (Step 1) and adding it to the result of the load	
	calculation (Step 2).	This the total memory required for the detection server to load and process the index.

Table 19-37 Example memory calculation for a multi-token index comprising a single \* .rdx file (continued)

Table 19-38 provides an example calculation if the index does not include multi-tokens. In this case you only need to determine how much memory is required to load the index.

**Table 19-38** Example memory calculation for a single-token index

Step	Action	Example
1	Multiply the number of *.rdx files by 2 GB (rounding up 1.9 to 2).	If the index comprises 3 files, then:  3 * . rdx files * 2 GB each = 6 GB required to load the index on the detection server.

# Remote EDM indexing

An EDM index maps the data you want to protect to the Exact Data profile. The typical EDM workflow for creating the EDM index is to upload the data source file to the Enforce Server, create the Exact Data profile, and index the data source. Instead of uploading the data source file to the Enforce Server for indexing, you can index the data source locally and securely using the Remote EDM Indexer.

See "About the Exact Data Profile and index" on page 371.

For example, if copying the confidential data source file to the Enforce Server presents a potential security or logistical issue, you can use the Remote EDM Indexer to create the cryptographic index directly on the data source host before moving the index to the Enforce Server. If you are upgrading to the latest Symantec Data Loss Prevention version you may want to use the Remote EDM Indexer to update your existing EDM indexes.

See "About the Remote EDM Indexer" on page 433.

See "About the SQL Preindexer" on page 433.

The Remote EDM Indexer is a standalone tool that lets you index the data source file directly on the data source host.

See "System requirements for remote EDM indexing" on page 434.

#### About the Remote EDM Indexer

The Remote EDM Indexer utility converts a data source file to an EDM index. The utility is similar to the local EDM Indexer used by the Enforce Server. However, the Remote EDM Indexer is designed for use on a computer that is not part of the Symantec Data Loss Prevention server configuration.

Using the Remote EDM Indexer to index a data source on a remote machine has the following advantages over using the EDM Indexer on the Enforce Server:

- It enables the owner of the data, rather than the Symantec Data Loss Prevention administrator, to index the data.
- It shifts the system load that is required for indexing onto another computer. The CPU and RAM on the Enforce Server is reserved for other tasks.

See "About the SQL Preindexer" on page 433.

See "Workflow for remote EDM indexing" on page 434.

## About the SQL Preindexer

You use the SQL Preindexer utility with the Remote EDM Indexer to run SQL queries against Oracle databases and pipe the resulting data to the Remote EDM Indexer for indexing.

See "System requirements for remote EDM indexing" on page 434.

The SQL Preindexer utility is installed in the \SymantecDLP\Protect\bin directory during installation of the Remote EDM Indexer. The SQL Preindexer utility generates an index directly from an Oracle SQL database. The SQL Preindexer processes the database query and passes it to the standard input of the Remote EDM Indexer utility.

To use the SQL Preindexer the data source must be relatively clean since the query result data is piped directly to the Remote EDM Indexer.

See "About the Remote EDM Indexer" on page 433.

## System requirements for remote EDM indexing

The Remote EDM Indexer runs on the Windows and Linux operating system versions that are supported for Symantec Data Loss Prevention servers. See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for more information about operating system support.

The SQL Preindexer supports Oracle databases and requires a relatively clean data source.

See "About the SQL Preindexer" on page 433.

The RAM requirements for using the Remote EDM Indexer vary according to the size of the data source being indexed and the number of multi-token columns in the data source.

See "Memory requirements for EDM" on page 421.

## Workflow for remote EDM indexing

This section summarizes the steps to index a data file on a remote machine and then use the index in Symantec Data Loss Prevention.

See "About the Exact Data Profile and index" on page 371.

Table 19-39 Steps to use the Remote EDM Indexer

Step	Action	Description
Step 1	Install the Remote EDM Indexer on a computer that is not part of the Symantec Data Loss Prevention system.	See "About installing and running the Remote EDM Indexer and SQL Preindexer utilities" on page 435.
Step 2	Create an Exact Data Profile on the Enforce Server to use with the Remote EDM Indexer.	On the Enforce Server, generate an EDM Profile template using the *.edm file name extension and specifying the exact number of columns to be indexed. See "Creating an EDM profile template for remote indexing" on page 436.
Step 3	Copy the Exact Data Profile file to the computer where the Remote EDM Indexer resides.	Download the profile template from the Enforce Server and copy it to the remote data source host computer.  See "Downloading and copying the EDM profile file to a remote system" on page 439.

Step	Action	Description
Step 4 Run the Remote EDM Indexer and create the index files.	If you have a cleansed data source file, use the RemoteEDMIndexer with the -data, -profile and -result options.	
	files.	If the data source is an Oracle database, use the SqlPreindexer and the RemoteEDMIndexer to index the data source directly with the -alias (oracle DB host), -username and -password credentials, and the -query string or -query_path
		See "Generating remote index files" on page 439.
Step 5 Copy the index files from the remote machine to the	Copy the resulting *.pdx and *.rdx files from the remote machine to the Enforce Server host at C:\SymantecDLP\Protect\index.	
	Enforce Server.	See "Copying and loading remote index files to the Enforce Server" on page 442.
Step 6 Load the index files into the		Update the EDM profile by loading the externally generated index.
	Enforce Server.	Submit the profile for indexing.
		See "Copying and loading remote index files to the Enforce Server" on page 442.
Step 7	Troubleshoot any problems	Verify that indexing is started and completes.
	that occur during the indexing process.	Check the system events for Code 2926 ("Created Exact Data Profile" and "Data source saved").
	The ExternalDataSource. <name>.rdx and *.pdx files are removed from the index directory and replaced by the file DataSource.51.1.rdx.</name>	
		See "Troubleshooting remote indexing errors" on page 447.
Step 8	Create policy with EDM	You should see the column data for defining the EDM condition.
C	condition.	See "Configuring the Content Matches Exact Data policy condition" on page 396.

Table 19-39 Steps to use the Remote EDM Indexer (continued)

## About installing and running the Remote EDM Indexer and SQL Preindexer utilities

The Remote EDM Indexer is installed from the same installation program as the other Symantec Data Loss Prevention components. The SQL Preindexer is installed automatically when you install the Remote EDM Indexer. Both utilities are run from the command line and are stored at /SymantecDLP/Protect/bin.

See "Generating remote index files" on page 439.

To install the Remote EDM Indexer, copy the ProtectInstaller.exe (Windows) or the ProtectInstaller.sh (Linux) file to the remote computer where the data to be indexed resides. When running the installer, choose to install the "Indexer"

only and no other components. The Linux installer for the Remote EDM Indexer is a program that you run from the command console.

See "Installing the Remote EDM Indexer (Windows)" on page 448.

See "Installing the Remote EDM Indexer (Linux)" on page 449.

Both the Remote EDM Indexer and the SQL Preindexer run from the command line. If you are on a Linux system, change users to the "protect" user before running the SQL Preindexer. (The installation program creates the "protect" user.)

See "Generating remote index files" on page 439.

Note: For two- and three-tier Data Loss Prevention installations, you should not install the Remote EDM Indexer on the same system that hosts a detection server. Refer to the Symantec Data Loss Prevention Installatio Guide for more information.

## Creating an EDM profile template for remote indexing

The EDM Indexer uses an Exact Data Profile when it runs to ensure that the data is correctly formatted. You must create the Exact Data Profile before you use the Remote EDM Indexer. The profile is a template that describes the columns that are used to organize the data. The profile does not need to contain any data. After creating the profile, copy it to the computer that runs the Remote EDM Indexer.

See "About the Exact Data Profile and index" on page 371.

#### To create an EDM profile for remote indexing

- From the Enforce Server administration console, navigate to the **Manage** > Data Profiles > Exact Data screen.
- Click Add Exact Data Profile. 2
- 3 In the **Name** field, enter a name for the profile.

In the Data Source field, select Use This File Name, and enter the name of the index file to create with the \*.edm extension.

You must select this option since you are only creating the profile template at this point. Later you will then index the profile with data source using the Remote EDM Indexer. Enter the file name of the data source you plan to create for remote EDM indexing. Be sure to name the data source file exactly the same as the name you enter here.

See "Uploading exact data source files to the Enforce Server" on page 383.

Once you have copied the generated remote index back to the Enforce Server, you use the Load Externally Generated Index option to load the remote index into the profile template

See "Copying and loading remote index files to the Enforce Server" on page 442.

5 In the **Number of Columns** text box, specify the number of columns in the data source to be indexed.

For remote EDM indexing purposes you must specify the exact Number of **Columns** the index is to have. Be sure to include the exact number of columns you specify here in the data source file.

See "Uploading exact data source files to the Enforce Server" on page 383.

- If the first row of the data source contains the column names, select the option Read first row as column names.
- In the Error Threshold text box, enter the maximum percentage of rows that can contain errors.
  - If, during indexing of the data source, the number of rows with errors exceeds the percentage that you specify here, the indexing operation fails.
- In the Column Separator Char field, select the type of character that is used in your data source to separate the columns of data.
- In the File Encoding field, select the character encoding that is used in your data source.
  - If Latin characters are used, select the ISO-8859-1 option. For East Asian languages, use either the UTF-8 or UTF-16 options.
- 10 Click **Next** to map the column headings from the data source to the profile.

11 In the Field Mappings section, map the Data Source Field to the System Field for each column by selecting the column name from the System Field drop-down list.

The **Data Source Field** lists the number of columns you specified at the previous screen. The System Field contains a list of standard column headings. If any of the column headings in your data source match the choices available in the System Field list, map each accordingly. Be sure that you match the selection in the **System Field** column to its corresponding numbered column in the Data Source Field.

For example, for a data source that you have specified in the profile as having three columns, the mapping configuration may be:

Data Source Field	System Field
Col 1	First Name
Col 2	Last Name
Col 3	Social Security Number

12 If a Data Source Field does not map to a heading value in the options available from the System Field column, click the Advanced View link.

In the Advanced View the system displays a Custom Name column beside the System Field column.

Enter the correct column name in the text box that corresponds to the appropriate column in the data source.

Optionally, you can specify the data type for the **Custom Name** you entered by selecting the data type from the **Type** drop-down list. These data types are system-defined. Click the **description** link beside the **Type** name for details on each system-defined data type.

- 13 If you intend to use the Exact Data Profile to implement a policy template that contains one or more EDM rules, you can validate your profile mappings for the template. To do this, select the template from the Check mappings against policy template drop-down list and click Check now. The system indicates any unmapped fields that the template requires.
- 14 Do not select any **Indexing** option available at this screen, since you intend to index remotely.
- 15 Click **Finish** to complete the profile creation process.

## Downloading and copying the EDM profile file to a remote system

#### Download and copy the EDM profile to the remote system

Configure an Exact Data Profile.

See "Creating an EDM profile template for remote indexing" on page 436.

2 Download the EDM profile by selecting the download profile link at the Manage > Data Profiles > Exact Data screen.

The system prompts you to save the EDM profile as a file. The file extension is \*.edm.

Save the file.

If the data source host computer where you intend to run the Remote EDM Indexer is available on the same subnet as the Enforce Server you can browse to that computer and select it as the destination. Otherwise, manually copy the profile to the remote system.

Use the profile to index the data source using the Remote EDM Indexer. See "Generating remote index files" on page 439.

## Generating remote index files

You use the command-line Remote EDM Indexer utility to generate an EDM index for importing to the Enforce Server. You can use the Remote EDM Indexer to index data source file that you have generated and cleansed. Or you can pipe the output from the SQL Preindexer to the standard input of the Remote EDM Indexer. The SQL Preindexer requires an Oracle DB data source and clean data.

When the indexing process completes, the Remote EDM Indexer generates several files in the specified result directory. These files are named after the data file that was indexed, with one file having the .pdx extension and another file with the .rdx extension. Note that indexing a large data file may generate multiple .rdx files with numbered extensions. For example: my edm.rdx.1, my edm.rdx.2 and so forth.

**Table 19-40** Options for generating remotes EDM indexes

Use case	Description	Remarks
Remote EDM Indexer with data source file.	Specify data source file, EDM profile, output directory.	Use when you have a cleansed data source file; use for upgrading to DLP 12.5.
		See "Remote indexing examples using data source file" on page 440.

Use case	Description	Remarks
Remote EDM Indexer with SQL Preindexer	Query DB and pipe output to stdin of Remote EDM Indexer.	Requires Oracle DB and clean data.  See "Remote indexing examples using SQL Preindexer" on page 441.

Table 19-40 Options for generating remotes EDM indexes (continued)

## Remote indexing examples using data source file

To use the Remote EDM Indexer to index a flat data source file you have generated and cleansed, you specify the local data source file name and path (-data), the local EDM profile file name and path (-profile), and the output directory for the generated index files (-result).

The syntax for using the Remote EDM Indexer to generate an index from a cleansed data source flat file is as follows:

```
RemoteEDMIndexer -data=<local data source filename and path>
-profile=<local *.edm profile file name and path>
-result=<local output directory for *.rdx and *pdx index files>
```

#### For example:

```
RemoteEDMIndexer -data=C:\EDMIndexDirectory\CustomerData.dat
-profile=C:\EDMIndexDirectory\RemoteEDMProfile.edm
-result=C:\EDMIndexDirectory\
```

This command generates an EDM index using the local data source flat file CustomerData.dat and the local RemoteEDMProfile.edm file that you generated and copied from the Enforce Server to the remote host, where \EDMIndexDirectory is the directory for placing the generated index files.

When the generation of the indexes is successful, the utility displays the message "Successfully created index" as the last line of output.

In addition, the following index files are created and placed in the -result directory:

- ExternalDataSource.CustomerData.pdx
- ExternalDataSource.CustomerData.rdx

If the index is large there may be more than one \*.rdx file. You copy these files to the Enforce Server and update the EDM profile using the remote index.

See "Remote EDM Indexer command options" on page 445.

## Remote indexing examples using SQL Preindexer

If your data source is an Oracle DB and has clean data you can index the data source directly using the SQL Preindexer with the Remote EDM Indexer.

The syntax is as follows:

```
SqlPreindexer -alias=<oracle connect string: //host:port/SID>
-username=<DB user> -password=<DB password> -query=<sql to run> |
RemoteEDMIndexer -profile=<*.edm profile file name and path>
-result=<output directory for index files>
```

#### For example:

```
SqlPreindexer -alias=@//myhost:1521/orcl -username=scott -password=tiger
-query="SELECT name, salary FROM employee" |
RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm -result=C:\EDMIndexDirectory\
```

With this command the SQL Preindexer utility connects to the Oracle database and runs the SQL guery to retrieve name and salary data from the employee table. The SQL Preindexer returns the result of the guery to stdout (the command console). The SQL query must be in quotes. The Remote EDM Indexer command runs the utility and reads the query result from the stdin console. The Remote EDM Indexer indexes the data using the ExportEDMProfile.edm profile as specified by the profile file name and local file path.

When the generation of the indexes is successful, the utility displays the message "Successfully created index" as the last line of output.

In addition, the utility places the following generated index files in the EDMIndexDirectory -result directory:

- ExternalDataSource.CustomerData.pdx
- ExternalDataSource.CustomerData.rdx

Here is another example using SQL Preindexer and Remote EDM Indexer commands:

```
SqlPreindexer -alias=@//localhost:1521/CUST -username=cust user -password=cust pword
-query="SELECT account id, amount owed, available credit FROM customer account" -verbose |
RemoteEDMIndexer -profile=C:\EDMIndexDirectory\CustomerData.edm
-result=C:\EDMIndexDirectorv\ -verbose
```

Here the SQL Preindexer command queries the CUST.customer account table in the database for the account id, amount owed, and avialble credit records. The result is piped to the Remote EDM Indexer which generates the index files based on the CustomerData.edm profile. The -verbose option is used for troubleshooting. As an alternative to the -query SQL string you can use the -query path option and specify the file path and name for the SQL query (\*.sql). If you do not specify a query or query path the entire DB is queried.

```
SqlPreindexer -alias=@//localhost:1521/cust -username=cust user -password=cust pwrd
-query path=C:\EDMIndexDirectory\QueryCust.sql -verbose |
RemoteEDMIndexer -profile=C:\EDMIndexDirectory\CustomerData.edm
-result=C:\EDMIndexDirectory\ -verbose
```

See "SQL Preindexer command options" on page 443.

## Copying and loading remote index files to the Enforce Server

The following files are created in the -result directory when you remotely index a data source:

- ExternalDataSource.<DataSourceName>.pdx
- ExternalDataSource.<DataSourceName>.rdx (there may be more than 1 if the index is large)

After you create the index files on a remote machine, the files must be copied to the Enforce Server, loaded into the previously created remote EDM profile, and indexed.

See "Creating an EDM profile template for remote indexing" on page 436.

#### To copy and load the files on the Enforce Server

- 1 Go to the directory where the index files were generated. (This directory is the one specified in the -result option.)
- 2 Copy all of the index files with .pdx and .rdx extensions to the index directory on the Enforce Server. This directory is located at \SymantecDLP\Protect\Index (Windows) or /var/SyantecDLP/index (Linux).
- From the Enforce Server administration console, navigate to the **Manage** > Policies > Exact Data screen.

This screen lists all the Exact Data Profiles in the system.

- 4 Click the name of the Exact Data Profile you used with the Remote EDM Indexer.
- 5 To load the new index files, go to the Data Source section of the Exact Data Profile and select Load Externally Generated Index.

In the Indexing section, select **Submit Indexing Job on Save**.

As an alternative to indexing immediately on save, consider scheduling a job on the remote machine to run the Remote EDM Indexer on a regular basis. The job should also copy the generated files to the index directory on the Enforce Server. You can then schedule loading the updated index files on the Enforce Server from the profile by selecting **Load Externally Generated Index** and Submit Indexing Job on Schedule and configuring an indexing schedule.

See "Use scheduled indexing to automate profile updates" on page 457.

Click Save. 7

## SQL Preindexer command options

On install the SQL Preindexer utility is available at \SymantecDLP\Protect\bin (Windows) and /SymantecDLP/Protect/bin (Linux).

The SQL Preindexer provides a command-line interface. The syntax for running the utility is as follows:

SqlPreindexer -alias=<0//oracle host:port/SID> -username=<DB user> [options]

Note the following about the arguments:

- The SQL Preindexer requires the -alias and -username arguments.
- If you omit the -password option, the user is prompted to enter it.
- If you use the -query option, the SQL query string must be in quotes.
- If you omit the -query option, the utility indexes the entire database.
- To query using wildcards, use the -qeury path option. The SQL Preindexer does not support the use of wildcards from the command line using the -query option. For example: "select \* from CUST DATA" does not work with -query; you must query each individual column field: "select cust ID, cust Name, cust SSN from CUST DATE." The query "select \* from CUST DATA" works using the -qeury path command.

See "Remote indexing examples using SQL Preindexer" on page 441.

Table 19-41 lists the command options for the SQL Preindexer.

Table 19-41 SQL Preindexer command options

Option	Summary	Description
-alias	Oracle DB connect string Required	Specifies the database alias that is used to connect to the database in the following format: @//oracle_DB_host:port/SID
		For example:
		-alias=@//myhost:1521/ORCL
		-alias=@//localhost:1521/CUST
-driver	Oracle JDBC driver class	Specifies the JDBC driver class, for example: oracle.jdbc.driver.OracleDriver.
-encoding	Character encoding (iso-8859-1)	Specifies the character encoding of the data to index. The default is iso-8859-1.
		Data with non-English characters should use UTF-8 or UTF-16.
-password	Oracle DB password	Specifies the password to the database.
		If this option is not specified, the password is read from stdin.
-query	SQL query	This option specifies the SQL query to perform. The statement must be enclosed in quotes.
		If you omit the <code>-query</code> option the utility indexes the entire database.
-query_path	SQL script	Specifies the file name and local path that contains a SQL query to run. Must be full path.
		This option can be used as an alternative to the <code>-query</code> option when the query is a long SQL statement.
-separator	Output column separator (tab)	Specifies whether the output column separator is a comma, pipe, or tab. The default separator is a tab.
		To specify a comma separator or pipe separator, enclose the separator character in quotation marks: ", " or "   ".
-subprotocol	Oracle thin driver	Specifies the JDBC connect string subprotocol (for example, oracle:thin).
-username	Oracle DB user	Specifies the name of the database user.
	Required	
-verbose	Print verbose output for debugging.	Displays a statistical summation of the operation when it is complete.
		See "Troubleshooting preindexing errors" on page 446.

## Remote EDM Indexer command options

On install, the Remote EDM Indexer utility is available at

\SymantecDLP\Protect\bin (Windows) and /SymantecDLP/Protect/bin (Linux).

If you are on Linux, change users to the "protect" user before running the Remote EDM Indexer. (The installation program creates the "protect" user.)

The Remote EDM Indexer provides a command line interface. The syntax for running the utility is as follows:

RemoteEDMIndexer -profile=<file \*.edm> -result=<out dir> [options]

Note the following about the syntax:

- The Remote EDM Indexer requires the -profile and -result arguments.
- If you use a flat data source file as input, you must specify the file name and local path using the -data option.
- The -data option is omitted when you use the SQL Preindexer to pipe the data to the Remote EDM Indexer.

See "Remote indexing examples using data source file" on page 440.

Table 19-42 describes the command options for the Remote EDM Indexer.

Table 19-42 Remote EDM Indexer command options

Option	Summary	Description
-data	Data source to be indexed (stdin)	Specifies the data source to be indexed. If this option is not specified, the utility reads data from stdin.
	Required if you use a flat file	Required if using data source file and not the SQL Preindexer.
-encoding	Character encoding of data to be indexed (ISO-8859-1)	Specifies the character encoding of the data to index. The default is ISO-8859-1.
		Use UTF-8 or UTF-16 if the data contains non-English characters.
-ignore_date	Ignore expiration date of the EDM profile	Overrides the expiration date of the Exact Data Profile if the profile has expired. (By default, an Exact Data Profile expires after 30 days.)
-profile	File containing the EDM profile	Specifies the Exact Data Profile to be used. This profile is the one that is selected by clicking the "download link" on the
	Required	Exact Data screen in the Enforce Server management console

Option	Summary	Description
-result	Directory to place the resulting indexes Required	Specifies the directory where the index files are generated.
-verbose	Display verbose output	Displays a statistical summation of the indexing operation when the index is complete.  See "Troubleshooting preindexing errors" on page 446.

Table 19-42 Remote EDM Indexer command options (continued)

## Troubleshooting preindexing errors

If you receive an error that the SQL Preindexer was unable to perform query or failed to prepare for indexing, verify that the -query string is in quotes. You can test your -query string by running only the SQL Preindexer command. If the command is correct the data queried from the database is displayed to the console as stdout.

You may encounter errors when you index large amounts of data. Often the set of data contains a data record that is incomplete, inconsistent, or inaccurate. Data rows that contain more columns than expected or incorrect column data types often cannot be properly indexed and are unrecognized.

The SQL Preindexer can be configured to provide a summary of information about the indexing operation when it completes. To do so, specify the verbose option when running the SQL Preindexer.

To see the rows of data that the Remote EDM Indexer did not index, adjust the configuration in the Indexer.properties file using the following procedure.

#### To record those data rows that were not indexed

- Locate the Indexer.properties file at \SymantecDLP\Protect\config\Indexer.properties (Windows) or /SymantecDLP/Protect/config/Indexer.properties (Linux).
- 2 Open the file in a text editor.
- 3 Locate the create error file property and change the "false" setting to "true."
- Save and close the Indexer.properties file.

The Remote EDM Indexer logs errors in a file with the same name as the data file being indexed and the .err suffix.

The rows of data that are listed in the error file are not encrypted. Safeguard the error file to minimize any security risk from data exposure.

See "About the SQL Preindexer" on page 433.

## Troubleshooting remote indexing errors

The Remote EDM Indexer displays a message that indicates whether the indexing operation was successful or not. If the Remote EDM Indexer successfully creates the index, the console displays the message "Successfully created index" as the last line of output. In addition, \*.pdx and one or more \*.rdx files are created in the -result directory.

The result depends on the error threshold that you specify in the EDM profile. Any error percentage under the threshold completes successfully. Detailed information about the indexing operation is available with the -verbose option.

See "Remote EDM Indexer command options" on page 445.

If the index generation is not successful, try these troubleshooting tips:

Table 19-43 Remote Indexer troubleshooting tips

Error	Symptom	Description
Index files not generated	Use the -verbose option in the command to reveal error message.	Specifying the verbose option when running the Remote EDM Indexer provides a statistical summary of information about the indexing operation after it completes. This information includes the number of errors and where the errors occurred.
"Failed to create index"	Verify file and path names.	Verify that you included the full path and proper file name for the -data file and the -profile file (* . edm). The paths must be
"Cannot compute index"		local to the host.
"Unable to generate index"		
"Destination is not a directory"	Directory path not correct.	Verify that you properly entered the full path to the destination directory for the required -result argument.
*.idx file instead of *.rdx file	Did not use -data argument	The -data option is required if you are using a data source file and not the SQL Preindexer. In other words, the only time you don't use the -data argument is when you are using the SQL Preindexer.
		If you run the Remote EDM Indexer without the <code>-data</code> option and no SQL Preindexer query, you get an <code>*.idx</code> and <code>*.rdx</code> file that cannot be used as for the EDM index. Rerun the index using the <code>-data</code> option or a SQL Preindexer <code>-query</code> or <code>-query-path</code> .

In addition, you may encounter errors when you index large amounts of data. Often the set of data contains a data record that is incomplete, inconsistent, or incorrectly formatted. Data rows that contain more columns than expected or incorrect data types often cannot be properly indexed and are unrecognized during indexing. The rows of data with errors cannot be indexed until those errors are corrected and the Remote EDM Indexer rerun. Symantec provides a couple of ways to get information about any errors and the ultimate success of the indexing operation.

To see the actual rows of data that the Remote EDM Indexer failed to index, modify the Indexer.properties file.

#### To modify the Indexer.properties file and view remote indexing errors

- Locate the Indexer.properties file at \SymantecDLP\Protect\config\Indexer.properties (Windows) or /opt/SymantecDLP/Protect/config/Indexer.properties (Linux).
- 2 To edit the file, open it in a text editor.
- 3 Locate the create error file property parameter and change the "false" value to "true."
- Save and close the Indexer.properties file.

The Remote EDM Indexer logs errors in a file with the same name as the indexed data file and with an .err extension. This error file is created in the logs directory.

The rows of data that are listed in the error file are not encrypted. Encrypt the error file to minimize any security risk from data exposure.

## Installing the Remote EDM Indexer (Windows)

The Remote EDM Indexer (Windows) is installed from the same installation program as the other Symantec Data Loss Prevention components.

See "About the Remote EDM Indexer" on page 433.

See "Installing the Remote EDM Indexer (Linux)" on page 449.

#### To install the Remote EDM Indexer on Windows

- Copy the ProtectInstaller 12.5.exe file to the remote machine where the data to be indexed resides.
- **2** Go to the directory where you copied the ProtectInstaller 12.5.exe installer. You may need to change the file permissions to access the file.

3 Run the installation program by double-clicking the file

ProtectInstaller 12.5.exe.

The installer files unpack and the Welcome screen displays.

- Click **Next** and then accept the Symantec Software License Agreement to continue.
- Select **Indexer** from the list of components that appears and click **Next**.
- On the **Select Destination Directory** screen, click **Next** to accept the default installation location (recommended).

Alternately, click **Browse** to navigate to a different installation location, then click Next.

7 Choose a Start Menu folder and then click **Next**.

The Installing screen appears and displays an installation progress bar.

Click **Finish** to complete the installation.

The files to uninstall the Remote EDM Indexer are located in the root level of the Symantec Data Loss Prevention installation directory. Follow this procedure to uninstall the utility on Windows.

#### To uninstall Remote EDM Indexer from a Windows system

On the computer where the Remote EDM Indexer is installed, locate and run (double-click) the \SymantecDLP\uninstall.exe program.

The uninstallation program begins and the Uninstall screen is displayed.

- 2 Click Next. When the uninstallation process is complete, the Uninstall Complete screen is displayed.
- 3 Click Finish to close the program.

## Installing the Remote EDM Indexer (Linux)

The Linux version of the Remote EDM Indexer provides a text-based command console option to install the product. The following procedure describes how to install the Remote EDM Indexer for Linux from the command line.

See "About the Remote EDM Indexer" on page 433.

See "Installing the Remote EDM Indexer (Windows)" on page 448.

#### To install the Remote EDM Indexer on Linux

- Log on to the Linux system as the root user.
- 2 Copy the ProtectInstaller 12.5.sh file to the /tmp directory on the computer.

3 Using a terminal session, change the directory to /tmp by typing:

```
cd /tmp
```

You may need to change permissions on the file before you can run the file. If so, type:

```
chmod 775 ProtectInstaller 12.5.sh
```

5 Once the file permissions have been changed you can run the ProtectInstaller 12.5.sh file, by typing:

```
./ProtectInstaller 12.5.sh -i console
```

Once the console mode installation launches, the Introduction step is displayed. For most circumstances, it is recommended to use the defaults during installation whenever possible. Press **Enter** to proceed to the next step.

- At the **Choose Install Set** step, specify the component to install. To install the Remote EDM Indexer, type the number beside the option and press **Enter**.
- At the **Install Folder** step, type the absolute path to the directory where you want to install the files. The default location can be selected by pressing **Enter**.
- At the **Pre-Installation Summary** step, review the installation configuration that you have selected. If you are satisfied with the selections, press **Enter** to begin the installation. Or, type back and press Enter until you reach the step you want to change.
- When the installation completes, press **Enter** to close the installer.

The files to uninstall the Remote EDM Indexer are located in the root level of the Symantec Data Loss Prevention installation directory. Follow this procedure to uninstall the utility on Linux.

#### To remove a Remote EDM Indexer from the command line

1 Log on as root and change to the Uninstall directory by typing:

```
cd /opt/SymantecDLP/Uninstall
```

2 Run the Uninstall program by typing:

```
./Uninstall -i console
```

3 Follow any on-screen instructions.

# **Best practices for using EDM**

EDM is the most accurate form of detection. It is also the most complex to set up and maintain. To ensure that your EDM policies are as accurate as possible, consider the recommendations in this section when you are implementing your EDM profiles and policies.

The following table provides a summary of the EDM policy considerations discussed in this chapter, with links to individual topics for more details.

**Table 19-44** Summary of EDM best practices

Best practice	Description
Ensure that the data source file contains at least one column of unique data.	See "Ensure data source has at least one column of unique data" on page 452.
Eliminate duplicate rows and blank columns before indexing.	See "Cleanse the data source file of blank columns and duplicate rows" on page 453.
To reduce false positives, avoid single characters, quotes, abbreviations, numeric fields with less than 5 digits, and dates.	See "Remove ambiguous character types from the data source file" on page 454.
Understand multi-token indexing and clean up as necessary.	See "Understand how multi-token cell matching functions" on page 454.
Use the pipe ( ) character to delimit columns in your data source.	See "Do not use the comma delimiter if the data source has number fields" on page 455.
Review an example cleansed data source file.	See "Ensure that the data source is clean for indexing" on page 456.
Map data source column to system fields to leverage validation during indexing.	See "Map data source column to system fields to leverage validation" on page 455.
Leverage EDM policy templates whenever possible.	See "Leverage EDM policy templates when possible" on page 456.
Include the column headers as the first row of the data source file.	See "Include column headers as the first row of the data source file" on page 456.
Check the system alerts to tune Exact Data Profiles.	See "Check the system alerts to tune profile accuracy" on page 457.
Use stopwords to exclude common words from matching.	See "Use stopwords to exclude common words from detection" on page 457.
Automate profile updates with scheduled indexing.	See "Use scheduled indexing to automate profile updates" on page 457.

Best practice	Description
Match on two or three columns in an EDM rule.	See "Match on 3 columns in an EDM condition to increase detection accuracy" on page 458.
Leverage exception tuples to avoid false positives.	See "Leverage exception tuples to avoid false positives" on page 459.
Use a where clause to detect records that meet a specific criteria.	See "Use a WHERE clause to detect records that meet specific criteria" on page 460.
Use the minimum matches field to fine tune EDM rules.	See "Use the minimum matches field to fine tune EDM rules" on page 460.
Consider using Data Identifiers in combination with EDM rules.	See "Combine Data Identifiers with EDM rules to limit the impact of two-tier detection" on page 460.
Include an email address field in the Exact Data Profile for profiled DGM.	See "Include an email address field in the Exact Data Profile for profiled DGM" on page 461.
Use profiled DGM for Network Prevent for Web identity detection	See "Use profiled DGM for Network Prevent for Web identity detection" on page 461.

**Table 19-44** Summary of EDM best practices (continued)

## Ensure data source has at least one column of unique data

EDM is designed to detect combinations of data fields that are globally unique. At a minimum, your EDM index must include at least one column of data that contains a unique value for each record in the row. Column data such as account number, social security number, and credit card number are inherently unique, whereas state or zip code are not unique, nor are names. If you do not include at least one column of unique data in your index, your EDM profile will not accurately detect the data you want to protect

Table 19-45 describes the various types of unique data to include in your EDM indexes, as well as fields that are not unique. You can include the non-unique fields in your EDM indexes as long as you have at least one column field that is unique.

Non-unique data
The following data fields are not unique:
■ First name
■ Last name
■ City
■ State
■ Zip code
■ Password
■ PIN number

Table 19-45 Examples of unique data for EDM policies

## Cleanse the data source file of blank columns and duplicate rows

The data source file should be as clean as possible before you create the EDM index, otherwise the resulting profile may create false positives.

When you create the data source file, avoid including empty cells or blank columns. Blank columns or fields count as "errors" when you generate the EDM profile. A data source error is either an empty cell or a cell with the wrong type of data (a name appearing in a phone number column). If the errors exceed the error threshold percentage for the profile (by default, 5%), the system stops indexing and displays an indexing error message.

The best practice is to remove blank columns and empty cells from the data source file, rather than increasing the error threshold. Keep in mind that if you have many empty cells, it may require a 100% error threshold for the system to create the profile. If you specify 100% as the error threshold, the system indexes the data source without checking for errors.

In addition, do not fill empty cells or blank fields with bogus data so that the error threshold is met. Adding fictitious or "null" data to the data source file will reduce the accuracy of the EDM profile and is strongly discouraged. Content you want to monitor should be legitimate and not null.

See "About cleansing the exact data source file" on page 373.

See "Preparing the exact data source file for indexing" on page 381.

See "Ensure that the data source is clean for indexing" on page 456.

## Remove ambiguous character types from the data source file

You cannot have extraneous spaces, punctuation, and inconsistently populated fields in the data source file. You can use tools such as Stream Editor (sed) and AWK to remove these items from you data source file or files before indexing them.

Table 19-46	Characters to avoid in the data source file
-------------	---

Characters to avoid	Explanation			
Single characters	Single character fields should be eliminated from the data source file. These are more likely to cause false positives, since a single character is going to appear frequently in normal communications.			
Abbreviations	Abbreviated fields should be eliminated from the data source file for the same reason as single characters.			
Quotes	Text fields should not be enclosed in quotes.			
Small numbers	Indexing numeric fields that contain less than 5 digits is not recommended because it will likely yield many false positives.			
Dates	Date fields are also not recommended. Dates are treated like a string, so if you are indexing a date, such as 12/6/2007, the string will have to match exactly. The indexer will only match 12/6/2007, and not any other date formats, such as Dec 6, 2007, 12-6-2007, or 6 Dec 2007. It must be an exact match.			

## Understand how multi-token cell matching functions

An EDM rule performs a full-text search against the message, checking each word (except those that are excluded by way of the columns you choose to match in the policy) for potential matches. The matching algorithm compares each individual word in the message with the contents of each token in the data profile.

If a cell in the data profile contains multiple words separated by spaces, punctuation, or alternative Latin and Chinese, Japanese, and Korean (CJK) language characters, the cell is a multi-token cell. The sub-token parts of a multi-token cell obey the same rules as single-token cells: they are normalized according to their pattern where normalization can apply.

If a cell contains a multi-token, the multi-token must match exactly. For example, a column field with the value "Joe Brown" is a multi-token cell (assuming multi-token matching is enabled). At run-time the processor looks to match the exact string "Joe Brown," including the space (multiple spaces are normalized to one). The system does not match on "Joe" and "Brown" if they are detected as single tokens.

In addition, multi-token cells are more computationally expensive than single-token cells. If the index includes multi-token cells, you must verify that you have enough memory to index, load, and process the EDM profile.

If multi-token matching is enabled, any punctuation that is next to a space is ignored. Therefore, punctuation before and after a space is ignored.

Lastly, do not change the WIP setting from "true" to "false" unless you are sure that is the result you want to achieve. You should only set WIP = false when you need to loosen the matching criteria, such as account numbers where formatting may change across messages. Make sure you test detection results to ensure you are getting the matches you expect.

See "Memory requirements for EDM" on page 421.

#### Do not use the comma delimiter if the data source has number fields.

Of the three types of column delimiters that you can choose from for separating the fields in the data source file (pipe, tab, or comma), the pipe or tab (default) is recommended. The comma delimiter is ambiguous and should not be used, especially if one or more fields in your data source contain numbers. If you use a comma-delimited data source file, make sure there are no commas in the data set other than those used as column delimiters.

Note: Although the system also treats the pound sign, equals sign, plus sign, semicolon, and colon characters as separators, you should not use these because like the comma their meaning is ambiguous.

## Map data source column to system fields to leverage validation

When you create the Exact Data Profile, you can validate how well the fields in your data source match against system-defined patterns for that field. For example, if you map a field to the credit card system pattern, the system will validate that the data matches the credit card system pattern. If it does not, the system will create an error for every record that contains an invalid credit card number. Mapping data source fields in your index to system-defined field patterns helps you ensure that the fields in your index meet the data type criteria.

If there is no corresponding system field to map to a data source column, consider creating a custom field to map data source column data. You can use the description field to annotate both system and custom fields.

See "Mapping Exact Data Profile fields" on page 389.

See "Creating and modifying Exact Data Profiles" on page 385.

## Ensure that the data source is clean for indexing

The following list summarizes a cleansed data source that is ready for indexing:

- It contains at least one unique column field.
- It is not a single-column data source; it has two or more columns.
- Empty cells and rows and blank columns are removed.
- Incomplete and duplicate records are removed.
- The number of faulty cells is below the default error rate (5%) for indexing.
- Bogus data is not used to fill in blank cells or rows.
- Improper and ambiguous characters are removed.
- Multi-tokens comply with space and memory requirements.
- Column fields are validated against the system-defined patterns that are available.
- Mappings are validate against policy templates where applicable.

See "Ensure data source has at least one column of unique data" on page 452.

See "Cleanse the data source file of blank columns and duplicate rows" on page 453.

See "Remove ambiguous character types from the data source file" on page 454.

See "Understand how multi-token cell matching functions" on page 454.

See "Map data source column to system fields to leverage validation" on page 455.

## Leverage EDM policy templates when possible

Symantec Data Loss Prevention provides several policy templates that implement EDM rules. The general recommendation is to use policy templates whenever possible when implementing EDM. If you do use a policy template for EDM, you should validate the index against the template when you configure the Exact Data Profile.

See "EDM policy templates" on page 370.

See "Creating and modifying Exact Data Profiles" on page 385.

### Include column headers as the first row of the data source file

When you extract the source data to the data source file, you should include the column headers as the first row in the data source file. Including the column headers will make it easier for you to identify the data you want to use in your policies.

The column names reflect the column mappings that were created when the exact data profile was added. If there is an unmapped column, it is called Col X, where **X** is the column number (starting with 1) in the original data profile.

If the Exact Data Profile is to be used for DGM, the file must have a column with a heading of email, or the DGM will not appear in the Directory EDM drop-down list (at the remediation page).

## Check the system alerts to tune profile accuracy

You should always review the system alerts after creating the Exact Data Profile. The system alerts provide very specific information about problems encountered when creating the profile, such as a SSN in an address field, which will affect accuracy.

## Use stopwords to exclude common words from detection

During detection the EDM process ignores words found in the stopwords file. Stopwords are common words that are excluding from matching. For example, the stopwords file contains common words such as articles, prepositions, and so forth. You can adjust the stopwords file by adding to or removing words from the file. It is recommended that you back up the original before changing it.

Stopword files are located at the following directory where the detection server running the index is installed: \SymantecDLP\Protect\config\stopwords. By default the system uses the stopwords en.txt file, which is the English language version. Other language stopword files are also located in this same directory. You can change the default stopword language file by updating the Lexer. StopwordLanguages property in the Advanced Server Settings screen of the Enforce Server.

See "Configuring Advanced Server Settings for EDM policies" on page 400.

## Use scheduled indexing to automate profile updates

When you configure an **Exact Data Profile**, you can set a schedule for indexing the data source file. Index scheduling lets you decide when you want to index the data source file. For example, instead of indexing the data source at the same time that you define the profile, you can schedule it for a later date. Alternatively, if you need to reindex the data source on a regular basis, you can schedule indexing to occur on a regular basis.

Before you set up an index schedule, consider the following:

- If you update your data sources occasionally (for example, less than once a month), generally there is no need to create a schedule. Index the data each time you update the data source.
- Schedule indexing for times of minimal system use. Indexing affects performance throughout the Symantec Data Loss Prevention system, and large data sources can take time to index.
- Index a data source as soon as you add or modify the corresponding exact data profile, and re-index the data source whenever you update it. For example, consider a scenario whereby every Wednesday at 2:00 P.M. you generate an updated data source file. In this case you could schedule indexing every Wednesday at 3:00 P.M., giving you enough time to cleanse the data source file and copy it to the Enforce Server.
- Do not index data sources daily as this can degrade performance.
- Monitor results and modify your indexing schedule accordingly. If performance is good and you want more timely updates, for example, schedule more frequent data updates and indexing.

Consider using scheduled indexing with remote EDM indexing to keep an EDM profile up to date. For example, you can schedule a cron job on the remote machine to run the Remote EDM Indexer on a regular basis. The job can also copy the generated index files to the index directory on the Enforce Server. You can then configure the Enforce Server to load the externally generated index and submit it for indexing on a scheduled basis.

See "About index scheduling" on page 374.

See "Scheduling Exact Data Profile indexing" on page 392.

See "Copying and loading remote index files to the Enforce Server" on page 442.

## Match on 3 columns in an EDM condition to increase detection accuracy

In a structured data format such as a database, each row represents one record, with each record containing related values for each column data field. Thus, for an EDM policy rule condition to match, all the data must come from the same row or record of data. When you define an EDM rule, you must select the fields that must be present to be a match. Although there is no limit to the number of columns you can select to match in a row (up to the total number of columns in the index, which is a maximum of 32), it is recommended that you match on at least 2 or 3 columns, one of which must be unique. Generally matching on 3 fields is preferred, but if one of the columns contains a unique value such as SSN or Credit Card number, 2 columns may be used

Consider the following example. You want to create an EDM policy condition based on an **Exact Data Profile** that contains the following 5 columns of indexed data:

- First Name
- Last Name
- Social security number (SSN)
- Phone Number
- **Email Address**

If you select all 5 columns to be included in the policy, consider the possible results based on the number of fields you require for each match.

If you choose "1 of the selected fields" to match, the policy will undoubtedly generate a large number of false positives because the record will not be unique enough. (Even if the condition only matches the SSN field, there may still be false positives because there are other types of nine-digit numbers that may trigger a match.).

If you choose "2 of the selected fields" to match, the policy will still produce false positives because there are potential worthless combinations of data: First Name + Last Name. Phone Number + Email Address. or First Name + Phone Number.

If you choose to match on 4 or all 5 of the column fields, you will not be able to exclude certain data field combinations because that option is only available for matches on 2 or 3 fields.

See "Leverage exception tuples to avoid false positives" on page 459.

In this example, to ensure that you generate the most accurate match, the recommendation is that you choose "3 of the selected fields to match." In this way you can reduce the number of false positives while using one or more exceptions to exclude the combinations that do not present a concern, such as First Name + Last Name + Phone Number

Whatever number of fields you choose to match, ensure that you are including the column with the most unique data, and that you are matching at least 2-column fields.

## Leverage exception tuples to avoid false positives

The EDM policy condition lets you define exception tuples to exclude combinations on data. You must select 2 or 3 columns to match to leverage exception tuples.

EDM allows detection based on any combination of columns in a given row of data (that is, N of M fields from a given record). It can trigger on "tuples," or specified sets of data types. For example, a combination of the first name and SSN fields could be acceptable, but a combination of the last name and SSN fields would not.

EDM also allows more complex rules such as looking for N of M fields, but excluding specified tuples. For example, this type of rule definition is required to identify incidents in violation of state data privacy laws, such as California SB 1386, which requires a first name and last name in combination with any of the following: SSN, bank account number, credit card number, or driver's license number.

While exception tuples can help you reduce false positives, if you are using several exception tuples, it may be a sign your index is flawed. In this case, consider redoing your index so you do not have to use so many excluded combinations to achieve the desired matches.

## Use a WHERE clause to detect records that meet specific criteria

Another configuration parameter of the EDM policy condition is the "Where" clause option. This option matches on the exact value you specify for the field you select. You can enter multiple values by separating each with commas. Using a WHERE clause to detect records that meet specific criteria helps you improve the accuracy of your EDM policies.

For example, if you wanted to match only on an Exact Data Profile for "Employees" with a "State" field containing certain states, you could configure the match where "State" equals "CA,NV". This rule then causes the detection engine to match a message that contains either CA or NV as content.

## Use the minimum matches field to fine tune EDM rules

The minimum matches field is useful for fine-tuning the sensitivity of an EDM rule. For example, one employee's first and last name in an outgoing email may be acceptable. However, 100 employees' first and last names is a serious breach. Another example might be a last name and social security number policy. The policy might allow an employee to send information to a doctor, but the sending of two last names and social security numbers is suspicious.

## Combine Data Identifiers with EDM rules to limit the impact of two-tier detection

When implementing EDM policies, it is recommended that you combine Data Identifiers (DIs) rules with the EDM condition to form compound policies. As reference, note that all system-provided policy templates that implement EDM rules also implement Data Identifier rules in the same policy.

Data Identifiers and EDM are both designed to protect personally identifiable information (PII). Including Data Identifiers with your EDM rules make your policies more robust and reusable across detection servers because unlike EDM rules Data Identifiers are executed on the endpoint and do not require two-tier detection. Thus,

if an endpoint is off the network, the Data Identifier rules can protect PII such as SSNs.

Data Identifier rules are also useful to use in your EDM policies while you are gathering and preparing your confidential data for EDM indexing. For example, a policy might contain the US SSN Data Identifier and an EDM rule for as yet unindexed or unknown SSNs.

## Include an email address field in the Exact Data Profile for profiled DGM

You must include the appropriate fields in the Exact Data Profile to implement profiled DGM.

See "Creating the exact data source file for profiled DGM" on page 380.

If you include the email address field in the Exact Data Profile for profiled DGM and map it to the email data validator, email address will appear in the Directory EDM drop-down list (at the remediation page).

## Use profiled DGM for Network Prevent for Web identity detection

If you want to implement DGM for Network Prevent for Web, use one of the profiled DGM conditions to implement identity matching. For example, you may want to use identity matching to block all web traffic for a specific users. For Network Prevent for Web, you cannot use synchronized DGM conditions for this use case.

See "Creating the exact data source file for profiled DGM" on page 380.

See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.

# Detecting content using Indexed Document Matching (IDM)

This chapter includes the following topics:

- Introducing Indexed Document Matching (IDM)
- Configuring IDM profiles and policy conditions
- Best practices for using IDM

# **Introducing Indexed Document Matching (IDM)**

You use Indexed Document Matching (IDM) to protect confidential information that is stored as unstructured data in documents and files. For example, you can use IDM to detect financial report data stored in Microsoft Office documents, merger and acquisition information stored in PDF files, and source code stored in text files. You can also use IDM to detect binary files, such as JPEG images, CAD designs, and multimedia files. In addition, you can use IDM to detect derived content such as text that has been copied from a source document to another file.

See "Supported forms of matching for IDM" on page 463.

See "About the Indexed Document Profile" on page 465.

## About using IDM

To use IDM you collect the documents and files that you want to protect and index them using the Enforce Server. During the indexing process the system uses an algorithm to fingerprint each file or file contents. You then create a policy that

contains one or more IDM conditions that reference the index. In production the system uses the same algorithm to fingerprint inbound files and file content. The system then compares the fingerprints against the index for matches.

For example, consider a document source you have collected that includes several confidential Microsoft Office documents (Word, Excel, PowerPoint) and image files (JPEG, BMP). You create an Indexed Document Profile and index the documents and files. You then configure the Content Matches Document Signature policy condition with a **Minimum Document Exposure** setting of 50%. The IDM policy and index are deployed to a detection server.

In production the detection server checks inbound files against the index for matches. In this case if an inbound text-based file that the system can crack contains 50% or more of content indexed from one of the source documents, the system records a match. And, if an inbound image file has the same binary signature as one of the files that has been indexed, the system records a match. The server performs exact file matching automatically even though the policy condition is configured for partial matching.

See "Types of IDM detection" on page 464.

See "About the Indexed Document Profile" on page 465.

## Supported forms of matching for IDM

IDM supports three forms of matching: exact file, exact file contents, and partial file contents. Detection servers support all three forms of matching. The DLP Agent for Windows supports exact file and exact file contents matching locally on the endpoint.

Table 20-1 summarizes the forms of matching by platform that IDM supports.

Forms of matching for IDM **Table 20-1** 

Type of matching	Description	Platform
Exact file	Match is based on the binary signature of the file.  See "Using IDM to detect exact files" on page 470.	Detection server DLP Agent for Windows
Exact file contents	Match is a 100% match of the extracted and normalized file contents.  See "Using IDM to detect exact and partial file contents" on page 471.	Detection server DLP Agent for Windows

Type of matching	Description	Platform
Partial file contents	Match of discrete passages of extracted and normalized file contents.	Detection server
	See "Using IDM to detect exact and partial file contents" on page 471.	

Table 20-1 Forms of matching for IDM (continued)

## Types of IDM detection

There are three types of IDM detection implementations: agent, server, and two-tier. The type you choose is based on your data loss prevention requirements.

Table 20-2 summarizes the three types of IDM detection.

**Table 20-2** Types of IDM detection

Туре	Description	Details
Agent IDM	The DLP Agent for Windows performs exact file and file contents matching locally on the endpoint.	See "Agent IDM detection" on page 464.
Server IDM	The detection server performs exact file matching, exact file contents matching, and partial file contents matching.	See "Server IDM detection" on page 465.
Two-tier IDM	The DLP Agent sends the data to the detection server for policy evaluation.	See "Two-tier IDM detection" on page 465.

## Agent IDM detection

With Agent IDM detection the DLP Agent for Windows evaluates documents locally in real time for exact file and exact file contents matches. Agent IDM lets lets you use the block, notify, and user cancel response rules on the endpoint with IDM policies.

See "Supported forms of matching for IDM" on page 463.

Agent IDM does not support partial file contents matching. If you want to use partial file contents matching on the endpoint, you must use two-tier detection.

See "Two-tier IDM detection" on page 465.

Agent IDM is enabled by default for a newly installed Endpoint Server. If you have upgraded, agent IDM is disabled. In this case, if you want to use agent IDM you must enable it and reindex your IDM profiles so that the endpoint index is generated and made available for download by DLP Agents.

See "Using agent IDM after upgrade to version 12.5" on page 494.

#### Server IDM detection

With server IDM detection the IDM index is deployed to one or more detection servers and all detection processing occurs on the server or servers. You can use server IDM to perform exact file matching and file contents matching. For file contents matching, you can choose to match file contents exactly (100%) or partially (10% to 90%) according to the Minimum Document Exposure set for the IDM condition.

See "Supported forms of matching for IDM" on page 463.

#### Two-tier IDM detection

If the server index is deployed to an Endpoint Server, the system uses two-tier detection to perform matching (assuming that two-tier detection is enabled). With two-tier IDM the DLP Agent sends the data to the Endpoint Server for matching against the server index. If two-tier detection is enabled for IDM, the server supports all forms of matching, including exact file, exact file contents, and partial file contents.

If you use two-tier detection for IDM on the endpoint, make sure you understand the performance implications of two-tier detection.

See "Two-tier detection for DLP Agents" on page 309.

## About the Indexed Document Profile

The Indexed Document Profile is the user-defined configuration for creating and generating IDM indexes. You define an Indexed Document Profile using the Enforce Server administration console. You reference the profile in one or more IDM policy rules or exceptions. The profile is reusable across policies: you can create one document profile and reference it in multiple policies. When you create the Indexed Document Profile, you have the option of indexing the document source immediately on save of the profile or at a scheduled time. However, you must index the document source before you can detect policy violations.

See "Creating and modifying Indexed Document Profiles" on page 479.

For example, consider a scenario where you want to create an IDM index to detect when exact versions of certain financial documents are found, or when passages or sections of the documents are exposed. When you define the Indexed Document Profile, you can upload the documents to the Enforce Server, or you can index the documents on a network file share. You can also use file name and file size filters in the document profile to include or ignore certain files during indexing.

See "About the indexing process" on page 466.

#### About the document data source

The document data source is the collection of documents you want to index and detect using IDM. The maximum size of the document data source that you can index is 2 GB, which translates to approximately 300,000 or 400,000 documents. The exact number of documents the system permits depends on the average extracted text size (per document source).

See "Preparing the document data source for indexing" on page 475.

For smaller document sets (50 MB or less), you can upload the source files to the Enforce Server using a ZIP file. For larger document sets (up to 2 GB), you can copy the source files to the host file system where the Enforce Server is installed, either encapsulated within a single ZIP file or as individual files. You can use FTP/S to transfer the files to the Enforce Server. Alternatively, you can use the **Remote** SMB Share feature to remotely index documents that are stored on a CIFS file share or WebDAV-enabled server that is accessible to the Enforce Server

See "About indexing remote documents" on page 467.

The document data source can contain any file type and any combination of files. If the system can crack the file, IDM detects file contents, either exactly or partially depending on the platform and the policy configuration. If the system cannot crack the file, IDM detects the exact file.

See "Supported forms of matching for IDM" on page 463.

## About the indexing process

The IDM indexer is a separate process that installs with and runs on the Enforce Server.

During indexing the system stores the document source at \SymantecDLP\Protect\documentprofiles (on Windows) or /var/SymantecDLP/documentprofiles (on Linux). After indexing, for security purposes the system deletes the document source files that you have uploaded to the Enforce Server.

The result of the indexing process is two separate indexes: one for detection servers (the server index) and one for DLP Agents (the endpoint index). Both indexes are generated regardless of whether or not you are licensed for Endpoint Prevent or Endpoint Discover. On the Enforce Server, the system stores both indexes in \SymantecDLP\Protect\index (on Windows) or /var/SymantecDLP/index (on Linux).

See "About the server and agent index files" on page 467.

For most IDM deployments there is no need to configure the indexer. If necessary you can configure key settings for the indexer using the file

\SymantecDLP\Protect\config\Indexer.properties.

## About indexing remote documents

Although the IDM indexing process is local to the Enforce Server, you can index documents that are remote to the Enforce Server using the Common Internet File System (CIFS) protocol or the Web-based Distributed Authoring and Versioning (WebDAV) protocol. To index documents remotely you use the Use Remote SMB **Share** option when you configure the Indexed Document Profile.

See "Creating and modifying Indexed Document Profiles" on page 479.

Using the CIFS protocol you can remotely index documents stored on one or more file shares in a Microsoft Windows-networked environment. To do this you provide the Universal Naming Convention (UNC) path to a shared network folder resource and index the documents stored in that folder or subfolders depending on the level of permission granted

See "Using the remote SMB share option to index file shares" on page 486.

WebDAV provides extensions to the HTTP 1.1 protocol that enable collaborative editing and management of files stored on remote web servers. You can index such documents remotely by exposing them to the Enforce Server using WebDAV. For example, you can use the remote SMB option with a UNC address and a WebDAV client to index Microsoft SharePoint or OpenText Livelink documents.

See "Using the remote SMB share option to index SharePoint documents" on page 487.

## About the server and agent index files

When you create an **Indexed Document Profile** and index a document data source, the system generates two index files, one for server and one for endpoint. Both indexes are generated regardless of whether or not you are licensed for a particular detection server or the DLP Agent.

See "About index deployment and logging" on page 469.

The server index is a binary file named DocSource.rdx. The server index supports exact file, exact file contents, and partial file contents matching. If the document data source is large, the server index may span multiple \*.rdx files.

The endpoint index is a secure, binary file named EndpointDocSource.rdx. The endpoint index supports exact file and exact file contents matching. The endpoint index is always one file.

See "Supported forms of matching for IDM" on page 463.

To create the index entries for exact file and exact file contents matching, the system uses the MD5 message-digest algorithm. This algorithm is a one-way hash function that takes as input a message of arbitrary length and produces as output a 128-bit message-digest or "fingerprint" of the input. If the message input is a text-based document that the system can crack, such as a Microsoft Word file, the system extracts 100% of the file contents, normalizes it by removing whitespaces, punctuation, and formatting, and creates an MD5 hash. Otherwise, if the message input is a file that the system cannot crack, such as an image file, small file, or unsupported file type, the system creates an MD5 hash based on the binary signature of the file

See "Using IDM to detect exact files" on page 470.

See "Using IDM to detect exact and partial file contents" on page 471.

In addition, for file formats the system can crack, the indexer creates hashes for discrete sections of content or text passages. These hashes are used for partial matching and are exclusive to the server index. The system uses a statistical sampling method to store hashed sections of partial content so that not all extractable text is indexed. The hash function ensures that the server index does not contain actual document content. To keep the size of the endpoint index file small, partial file contents hashes are not included in the endpoint index.

Table 20-3 summarizes the types of matching supported by the endpoint and server indexes.

Table 20-3	Types of	f matching	g supported	l by the end	point and	l server indexes

Message input	Output	Matches	Included in index file
	A single MD5 hash derived from 100% of the extracted and normalized file contents	Exact file contents (100%)	DocSource.rdx EndpointDocSource.rdx
Text-based file that the system can crack	One or more rolling hashes based on discrete passages of extracted and normalized content using a statistical sampling method of selection	Partial file contents (10% to 90%)	DocSource.rdx
Binary file, custom file, small file, encapsulated file	A single MD5 hash based on the binary signature of the file	Exact file binary	DocSource.rdx EndpointDocSource.rdx

#### About index deployment and logging

The Enforce Server is responsible for deploying the IDM server and endpoint indexes to the detection and Endpoint Servers. You cannot manually deploy the indexes.

The system deploys the server index to each designated detection server in the folder \SymantecDLP\Protect\index (on Windows) or /var/SymantecDLP/index (on Linux). At run-time, the detection server loads the server index into random access memory (RAM) when an active IDM policy that references that index is deployed to that detection server.

The system deploys the endpoint index to each designated Endpoint Server. When a DLP Agent connects to the Endpoint Server, the DLP Agent downloads the endpoint index. Assuming agent IDM is enabled, the DLP Agent loads the endpoint index into memory when the index is required by an active local policy. The endpoint index is much smaller in size than the server index so there is no degradation in endpoint performance.

See "Estimating endpoint memory use for agent IDM" on page 496.

You cannot manually deploy either the sever or endpoint index files by copying the \*.rdx file or files from the Enforce Server to a detection server. The detection server does not monitor the index destination folder for new index files: the detection server must be notified by the Enforce Server that an index has been deployed. If a detection server is offline during the index deployment process, the Enforce Server will cease trying to deploy the index. When the detection server comes back online the Enforce Server will deploy the index to the detection server. The same is true for DLP Agents. There is now way to manually copy the endpoint index to the endpoint host and have the DLP Agent recognize the index.

Table 20-4 summarizes how IDM indexes are deployed and the logs files to check to troubleshoot index deployment.

	Table 20-4	IDM index deployment and logging	
Index file		Deployment	Logge

Platform	Index file	Deployment	Logged
Server	DocSource.rdx	Sent automatically by the Enforce Server to each designated detection server after the index is generated. Loaded by the detection server into RAM at run-time.	detection_operational.log Use to identify if the index profile was deployed to the detection server. FileReader.log Use to to see if the index profile is loaded into memory.

Platform	Index file	Deployment	Logged
Agent	EndpointDocSource.rdx	Sent by the Enforce Server to each designated Endpoint Server.  Downloaded by the DLP Agent based on the agent connection interval.  Loaded into RAM at run-time when a local, active policy requires the index.	endpoint_server_operational.log Use to identify if the index profile was deployed to the Endpoint Server. Pull the agent logs to see if the index profile is loaded into memory.

Table 20-4 IDM index deployment and logging (continued)

#### Using IDM to detect exact files

The system performs exact file matching automatically on all binary files. In addition, if the file format is text-based but the system is unable to crack the file and extract file contents, the system performs exact file matching. This behavior is true even if you select a **Minimum Document Exposure** percentage for the IDM condition that is less than Exact.

See "About the server and agent index files" on page 467.

For example, an IDM rule with a minimum document exposure set to 50% automatically attempts to match a binary file exactly because the **Minimum** Document Exposure setting only applies to crackable files. In addition, the system performs exact file matching for files containing a very small amount of text, as well as files that were encapsulated when indexed, even if text-based.

As an optimization, for exact file type matching, the system checks the byte size of the file before computing the run-time hash for comparison against the index. If the byte size does not match size of the indexed file there is no need to compute the exact file hash. The system does not consider the file format when creating the exact file fingerprint.

Table 20-5 summarizes exact file type matching behavior.

**Table 20-5** Requirements for using IDM to detect files

File format	Example	Description
Text-based file format the system cannot crack	Proprietary or non-supported document format	If the system cannot crack the file format, you can use IDM to detect that specific file using exact binary matching.
		See "Do not compress files in the document source" on page 500.

File format	Example	Description
Binary file	GIF, MPG, AVI, CAD design, JPEG files, audio/video files	You can use IDM to detect binary file types that cannot be cracked, such as images, graphics, JPEGs, etc.  See "Avoid using IDM solely for binary files" on page 501.
File containing a small amount of text	CAD files, Visio diagrams, and so on	A file containing a small amount of text will be treated as a binary file even if the contents are text-based and crackable.  See "Using IDM to detect exact and partial file contents" on page 471.
Encapsulated file	Any file that is encapsulated when indexed (even if text-based and crackable); for example, Microsoft Word file archived in a ZIP file	If a document data source file is encapsulated in an archive file, the file contents of the subfile cannot be extracted and only the binary signature of the file can be fingerprinted. This does not apply to the main document archive that contains all documents to be indexed.
		See "About the document data source" on page 466.

**Table 20-5** Requirements for using IDM to detect files (continued)

#### Using IDM to detect exact and partial file contents

The primary use case for IDM is to detect file contents (as distinguished from binary files, such as audio or video files, for example). On the server you can use IDM to match file contents exactly (100%) or partially (10% to 90%). On the endpoint you can use IDM to match file contents exactly. File contents include text-based content of any document type the system can crack, such as Microsoft Office documents (Word, Excel, PowerPoint), PDF, and many more.

See "Supported formats for content extraction" on page 684.

An exact file contents match means that 100% of the inbound file contents matches exactly the content of a file that has been indexed. The system does not consider the file format or file size when creating the MD5 hash for the index or when checking for an exact file contents match against the index. A document might contain much more content, but the system detects only the file contents that are indexed as part of the Indexed Document Profile. For example, consider a situation where you index a one-page document, and that one-page document is included as part of a 100-page document. The 100-page document is considered a 100% match because its content matches the one-page document exactly.

See "About the server and agent index files" on page 467.

Partial file contents matching only applies to server-based IDM indexes. For text-based files that are crackable, in addition to creating the MD5 fingerprint for exact file contents matching, the system uses a rolling hash algorithm to register discrete sections or passages of content. In this case the system uses a statistical sampling method to store hashed sections of content; not all text is hashed in the index. The index does not contain actual document content.

Table 20-6 lists the requirements to match file contents using IDM.

Requirements for using IDM to detect content Table 20-6

	Table 20-0 Requirements for using 10 M to detect content
Requirement	Description
Crackable file format	The system must be able to crack the file format and extract file content. Data Loss Prevention supports context extraction for over 100 file types.
	See "Supported formats for content extraction" on page 684.
Natural file state	To match file contents, the source file cannot be encapsulated in an archive file when the source file is indexed. If a file in the document source is encapsulated in an archive file, the system does not index the file contents of the encapsulated file. Any encapsulated file is considered for exact matches only, like image files and other unsupported file formats.
	See "Do not compress files in the document source" on page 500.
	<b>Note:</b> The exception to this is the main ZIP file that contains the document data source, for those upload methods that use an archive file. See "Creating and modifying Indexed Document Profiles" on page 479.
Minimum amount of text	For exact file contents matching, the source file must contain at a minimum 30 characters of normalized text before the cracked content is indexed. Normalization involves the removal of punctuation and whitespaces. A normalized character therefore is either a number or a letter. This size is set by the min_normalized_size=30 parameter in the file \SymantecDLP\Protect\config\Indexer.properties. If file contents is less than 30 normalized characters, the system performs an exact file match against the file binary.
	For partial file contents matching, there must be at least 130 normalized characters. However, the exact length is variable depending on the file contents and encoding.
	See "Do not index empty documents" on page 501.
Maximum amount of text	The maximum size of the document that can be processed for content extraction at run-time is 30 MB. If a file is larger than this, only the first 30 MB of content is extracted for indexing.
	For example, consider a file that is 50 MB. During indexing an MD5 will be created for the entire 50 MB. During detection, the file would be truncated to 30 MB. Further, the text would still be extracted, assuming it can be. The result would be no match since the index only has an MD5 for the 50 MB and detection would generate fingerprints on the text and an MD5 for the first 30 MB
	See "Advanced server settings" on page 203.

#### About using the Content Matches Document Signature policy condition

You use the IDM condition Content Matches Document Signature From to implement IDM detection rules and exceptions in your policies.

See "Configuring the Content Matches Document Signature policy condition" on page 497.

When you configure this condition, you specify the IDM index to use and how the condition should match against the index using the Minimum Document Exposure setting. You can select either Exact or partial between 10% to 90%. For example, if you select 70% for the Minimum Document Exposure, a match occurs only if 70% or more of the hashed file contents is detected.

See "Use parallel IDM rules to tune match thresholds" on page 507.

If a file is not text-based, is not crackable, is very small, or is encapsulated in an archive file, the file is matched exactly based on its binary signature. This form of matching is performed automatically by the system, regardless of what configuration option you choose for the Minimum Document Exposure setting. This setting only applies to partial file contents matching.

See "Using IDM to detect exact files" on page 470.

Table 20-7 describes the matching supported by the Content Matches Document Signature From policy condition.

Table 20-7 Minimum document exposure settings for the IDM condition

Configuration setting	File type	Match	Example
Exact matching	File contents See "Using IDM to detect exact and partial file contents" on page 471.	100% of the extracted and normalized file contents, if the file is text-based and crackable	Microsoft Word
Partial (10% to 90%)	File contents  See "Using IDM to detect exact and partial file contents" on page 471.	Discrete passages of text	Microsoft Word
Automatic	File See "Using IDM to detect exact files" on page 470.	Binary signature of the file, if the file is not text-based or is not crackable	JPEG, small file, custom file, archived subfile

#### About using IDM for policy exceptions

You can use the IDM policy condition Content Matches Document Signature From as an exception to exclude specific documents from exact matching. You cannot use the IDM policy condition to except content from matching. To exclude content in documents from matching, you need to "whitelist" it.

See "About whitelisting partial file contents" on page 474.

As an example of using the IDM condition for policy exceptions, consider a data source that you index which contains JPEG files. You create a policy that contains two conditions: one rule implements a file type match condition on the JPEG file format; and an exception implements the IDM condition that references the IDM index containing JPEG files. At run-time any JPEG file detected triggers an incident, except one that matches an MD5 fingerprint in the index.

For an additional example on how to implement IDM as a policy exception, refer to the CAN-SPAM Act policy template that is included with installation of Data Loss Prevention.

See "CAN-SPAM Act policy template" on page 805.

## About whitelisting partial file contents

Often sensitive documents contain standard boilerplate text that that does not require protection, including front matter, headers, and footers. Information contained in document headers and footers is likely to cause false positives. Likewise, boilerplate text, such as standard language and non-proprietary corporate content that is repeated across confidential documents, can cause false positives.

See "Whitelisting file contents to exclude from partial matching" on page 476.

Removing non-sensitive boilerplate or header/footer content before indexing is usually not feasible, especially if you have a large document data set. In this case you can configure the system to exclude ("whitelist") non-sensitive text. You do this by adding the text to ignore to the whitelist file. During indexing, any whitelisted content found in the source files is ignored. At run-time the content will not cause false positives because it has been excluded.

See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.

Note: Whitelisting only applies to partial file contents matching; it does not apply to exact file contents matching. The whitelisting file is not checked at run-time when the system computes the MD5 hashes for exact file contents matching.

# Configuring IDM profiles and policy conditions

Table 20-8 provides the workflow for creating IDM profiles and configuring IDM policies. Complete the steps to ensure that your IDM rules are properly implemented and are as accurate and efficient as possible.

**Table 20-8** Implementing IDM

Step	Action	Description
1	Identify the content you want to protect and collect the documents that contain this	See "Using IDM to detect exact and partial file contents" on page 471.
	content.	See "Using IDM to detect exact files" on page 470.
2	Prepare the documents for indexing.	See "Preparing the document data source for indexing" on page 475.
3	Whitelist headers, footers, and boilerplate text.	See "Whitelisting file contents to exclude from partial matching" on page 476.
4	Create an Indexed Document Profile and specify the document source.	See "Creating and modifying Indexed Document Profiles" on page 479.
5	Configure any document source filters.	See "Filtering documents by file name" on page 489.
6	Schedule indexing as necessary.	See "Scheduling document profile indexing" on page 492.
7	Configure one ore more IDM policy conditions or exceptions.	See "Configuring the Content Matches Document Signature policy condition" on page 497.
8	Test and troubleshoot your IDM implementation.	See "Troubleshooting policies" on page 353.

#### Preparing the document data source for indexing

You must collect and prepare the documents you want to index. These documents are known as the document data source.

See "About the document data source" on page 466.

A document data source is a ZIP archive file that contains the documents to index. It can also be the files stored in a file share on a local or remote computer. If you have a file share that already contains the documents you want to protect, you can reference this share in the document profile.

A document data source is a ZIP archive file that contains the documents to index. It can also be the files stored in a file share on a local or remote computer. A document data source ZIP file can contain any file type and any combination of

files. If you have a file share that already contains the documents you want to protect, you can reference this share in the document profile.

**Table 20-9** Preparing the document source for indexing

Step	Action	Description
1		Collect all of the documents you want to index and put them in a folder.
	you want to protect.	See "About the document data source" on page 466.
2	Uncompress all the files you want to index.	The files you index should be in their natural, uncompressed state. Check the document collection to make sure none of the files are encapsulated in an archive file, such as ZIP, TAR, or RAR. If a file is embedded in an archive file, extract the source file from the archive file and remove the archive file. See "Using IDM to detect exact and partial file contents" on page 471.
3	Separate the documents if you have more than 2 GB to index.	To protect a large amount of content and files, create separate collections for each set of documents over 2 GB in size, with all files in their natural, uncompressed state. For example, if you have 3 GB of documents you want to index, separate the files by folders, one folder containing 2 GB of data, and another folder containing the remaining 1 GB of data.  See "Create separate profiles to index large document sources" on page 505.
4	Decide how you are going to make the document source files available to the Enforce Server.	The indexing process is a separate process that runs on the Enforce Server. To index the document source you must make the files accessible to the Enforce Server. You have several options. Decide which one works best for your needs and proceeding accordingly.  See "Uploading a document archive to the Enforce Server" on page 482.  See "Referencing a document archive on the Enforce Server" on page 483.
		See "Using local path on Enforce Server" on page 485.  See "Using the remote SMB share option to index file shares" on page 486.
5	Configure the document profile.	The next step is to configure the document profile, or, alternatively, if you want to exclude specific document content from detection, whitelist it.
		See "Creating and modifying Indexed Document Profiles" on page 479.
		See "Whitelisting file contents to exclude from partial matching" on page 476.

## Whitelisting file contents to exclude from partial matching

You use whitelisting to exclude unimportant or noncritical content, such as standard boilerplate text, document headers and footers, from the IDM index. Whitelisting such content helps to reduce false positives.

See "About whitelisting partial file contents" on page 474.

See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.

To exclude content from matching, you copy the content you want to exclude to a text file and save the file as Whitelisted.txt. By default, the file must contain at least 130 non-whitespace characters to have its content fingerprinted for whitelisting purposes. When you index the document source, the Enforce Server looks for the Whitelisted.txt file.

See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.

Table 20-10 describes the process for excluding document content using whitelisting.

Table 20-10 Whitelisting non-sensitive content

Step	Action	Description
1	Copy the content you want to exclude from matching into a text file.	Copy only noncritical content you want to exclude, such as standard boilerplate text and document headers and footers, to the text file. By default, for file contents matching the file to be indexed must contain at least 130 characters. This default setting applies to the Whitelisted.txt file as well. For whitelisted text you can change this default setting.  See "Changing the default indexer properties" on page 493.
2	Save the text file as Whitelisted.txt.	The Whitelisted.txt file is the source file for storing content you want to exclude from matching.
3	Save the file to the whitelisted directory on the Enforce Server host file system.	Save the file to \SymantecDLP\Protect\documentprofiles\whitelisted(on Windows) or \var/SymantecDLP/documentprofiles/whitelisted(on Linux).
4	Configure the Indexed  Document Profile and generate the index.	When you index the document data source, the Enforce Server looks for the <code>Whitelisted.txt</code> file. If the file exists, the Enforce Server copies it to <code>Whitelisted.x.txt</code> , where x is a unique identification number corresponding to the <code>Indexed Document Profile</code> . Future indexing of the profile uses the profile-specific <code>Whitelisted.x.txt</code> file, not the generic <code>Whitelisted.txt</code> file.  See "Creating and modifying <code>Indexed Document Profiles</code> " on page 479.

## Manage and add Indexed Document Profiles

The Manage > Data Profiles > Indexed Documents screen lists all configured Indexed Document Profiles in the system. From this screen you can manage existing profiles and add new ones.

**Table 20-11** Indexed Documents screen actions

Column	Description
Add IDM profile	Click Add Document Profile to create a new Indexed Document Profile.
	See "Configuring IDM profiles and policy conditions" on page 475.
Edit IDM profile	Click the name of the Document Profile, or click the pencil icon to the far right of the profile, to modify an existing Document Profile.
	See "Creating and modifying Indexed Document Profiles" on page 479.
Remove IDM profile	Click the red X icon next to the far right of the document profile row to delete that profile from the system. A dialog box confirms the deletion.
	<b>Note:</b> You cannot edit or remove a profile if another user currently modifies that profile, or if a policy exists that depends on that profile.
Refresh IDM profile status	Click the refresh arrow icon at the upper right of the <b>Indexed Documents</b> screen to fetch the latest status of the indexing process. If you are in the process of indexing, the system displays the message "Indexing is starting." The system does not automatically update the screen when the indexing process is complete.

**Table 20-12** Indexed Documents screen details

Column	Description	
Document Profile	The name of the Indexed Document Profile.	
Detection server	The name of the detection server that indexes the Document Profile and the Document Profile version.	
	Click the triangle icon beside the Document Profile name to display this information. It appears beneath the name of the Document Profile.	
Location	The location of the file(s) on the Enforce Server that the system has profiled and indexed.	
Documents	The number of documents that the system has indexed for the document profile.	

Table 20-12 Indexed Documents screen details (continued)

Column	Description
Status	The current status of the document indexing process, which can be any of the following:  Next scheduled indexing (if it is not currently indexing)  Sending an index to a detection server  Indexing  Deploying to a detection server
	In addition, beneath the status of the indexing process, the system displays the status of each detection server, which can be any of the following:  Completed, including a completion date Pending index completion (that is, waiting for the Enforce Server to finish indexing a file) Replicating indexing Creating index (internally) Building caches
Error messages	The <b>Indexed Document</b> screen also displays any error messages in red (for example, if the document profile is corrupted or does not exist).

See "Data Profiles" on page 291.

See "Scheduling document profile indexing" on page 492.

See "Configuring the Content Matches Document Signature policy condition" on page 497.

#### Creating and modifying Indexed Document Profiles

You define and configure an Indexed Document Profile at the screen Manage > Data Profiles > Indexed Documents > Configure Document Profile. The document profile specifies the document data source, the indexing parameters, and the indexing schedule. You must define a document profile to implement IDM detection.

See "About the Indexed Document Profile" on page 465.

Table 20-13 describes the steps for creating and modifying IDM profiles.

Configuring a document profile **Table 20-13** 

Step	Action	Description
1	Navigate to the screen Manage > Data Profiles > Indexed Documents.	You must be logged on to the Enforce Server administration console as an administrator or policy author.
		See "Policy authoring privileges" on page 290.
2	Click Add Document Profile.	Select an existing Indexed Document Profile to edit it.
		See "Manage and add Indexed Document Profiles" on page 477.
3	Enter a <b>Name</b> for the Document Profile.	Choose a name that describes the data content and the index type (for example, "Research Docs IDM"). The name is limited to 255 characters.
		See "Input character limits for policy configuration" on page 344.

Configuring a document profile (continued) Table 20-13

Step	Action	Description
4	Select the <b>Document Source</b> method for indexing.	Select one of the four options for indexing the document data source, depending on how large your data source is and how you have packaged it.
		See "About the document data source" on page 466.
		Options for making the data source available to the Enforce Server.
		<ul> <li>Upload Document Archive to Server Now         To use this method, you Browse and select a ZIP file containing the documents to be indexed. The maximum size of the ZIP file is 50 MB.         See "Uploading a document archive to the Enforce Server" on page 482.     </li> <li>Reference Archive on Enforce Server         Use this method if you have copied the ZIP file to the file system host where the Enforce Server is installed. The maximum size of the ZIP file is 2 GB. This ZIP file is available for selection in the drop-down field.         See "Referencing a document archive on the Enforce Server" on page 483.     </li> <li>Use Local Path on Enforce Server         This method lets you index individual files that are local to the Enforce Server. With this method the files to be indexed cannot be archived in a ZIP file. The maximum size of the documents that can be indexed is 2 GB.         See "Using local path on Enforce Server" on page 485.     </li> <li>Use Remote SMB Share         See "About indexing remote documents" on page 467.         See "Using the remote SMB share option to index file shares" on page 486.         See "Using the remote SMB share option to index SharePoint documents" on page 487.     </li> </ul>

table 20-10 companing a decament prome (continues)			
Step	Action	Description	
5	Optionally, configure any <b>Filters</b> .	You can specify file name and file size filters in the document profile. The filters tell the system which files to include or ignore during indexing.	
		See "Filter documents from indexing to reduce false positives" on page 504.	
		Enter files to include in the <b>File Name Include Filters</b> field, or enter files to exclude in the <b>File Name Exclude Filters</b> field.	
		See "Filtering documents by file name" on page 489.	
		Select file sizes to ignore, either <b>Ignore Files Smaller Than</b> or <b>Ignore Files Larger Than</b> .	
		See "Filtering documents by file size" on page 491.	
6	Select one of the <b>Indexing</b> options.	As part of creating a document profile, you can set up a schedule for indexing the document source.	
		You do not have to select an indexing option to create a profile that you can reference in a policy, but you must select an indexing option to generate the index and actually detect matches using an IDM policy.	
		Select Submit Indexing Job on Save to index the document source immediately on save of the Document Profile.  Select Submit Indexing Job on Save to index the document source immediately on save of the Document Profile.	
		Select Submit Indexing Job on Schedule to display schedule options so that you can schedule indexing at a later time. See "Scheduling document profile indexing" on page 492.	
7	Click Save.	You must save the document profile.	

Table 20-13 Configuring a document profile (continued)

## Uploading a document archive to the Enforce Server

The Upload Document Archive to Server Now option lets you upload a ZIP file with a maximum size of 50 MB to the Enforce Server and index its contents. To use this method of indexing, the document source must meet the requirements described in the table Table 20-14

To upload the document archive to Enforce Server describes the process for using the Upload Document Archive to Server Now method of indexing.

#### To upload the document archive to Enforce Server

- Navigate to the screen Manage > Data Profiles > Indexed Documents > Configure Document Profile.
- 2 Select the option Upload Document Archive to Server Now.

Click **Browse** and select the ZIP file. The ZIP file can be anywhere on the same network as the Enforce Server.

Optionally, you can type the full path and the file name if the ZIP file is local to the Enforce Server, for example: c:\Documents\Research.zip.

Specify one or more file name or file size filters (optional).

See "Filtering documents by file name" on page 489.

Select one of the indexing options (optional).

See "Scheduling document profile indexing" on page 492.

5 Click Save.

Table 20-14 Requirements for using the Upload Document Archive to Server Now option

Requirement	Description
ZIP file only	The document archive must be a ZIP file; no other encapsulation formats are supported for this option.
50 MB or less	You cannot use this option if the document archive ZIP file is more than 50 MB because files exdeeding that size limit can take too long to upload and slow the performance of the Enforce Server. If the document archive ZIP file is over 50 MB, use the <b>Reference Archive on Enforce Server</b> method instead.
UTF-8 file names only	The IDM indexing process fails (and presents you with an "unexpected error") if the document archive (ZIP file) contains non-ASCII file names in encodings other that UTF-8.
	If the ZIP file contains files with non-ASCII file names, use either of the following options instead to make the files available to the Enforce Server for indexing:
	<ul><li>Use Local Path on Enforce Server</li><li>Use Remote SMB Share</li></ul>

#### Referencing a document archive on the Enforce Server

You use the Reference Archive on Enforce Server option to create an IDM index based on a ZIP file that is local to the Enforce Server. You use this option to index source documents that are archived in a ZIP file that is larger than 50 MB.

See "About the document data source" on page 466.

Note: If the ZIP file is less than 50 MB, you can use the Upload Document Archive to Server Now option instead. See "Uploading a document archive to the Enforce Server" on page 482.

To use the Reference Archive on Enforce Server option, you copy the ZIP file to the \SymantecDLP\Protect\documentprofiles folder on the Enforce Server file system host. Once you have copied the ZIP file to the Enforce Server, you can select the document source from the pull-down menu at the Add Document Profile screen. See "Creating and modifying Indexed Document Profiles" on page 479.

To reference the document archive on the Enforce Server describes the procedure for using the Reference Archive on Enforce Server option.

#### To reference the document archive on the Enforce Server

- Copy the ZIP file to the Enforce Server.
  - On Windows, copy the ZIP file to directory \SymantecDLP\Protect\documentprofiles
  - On Linux, copy the ZIP file to directory /var/SymatnecDLP/documentprofiles

See Table 20-15 on page 485.

Note: The system deletes the document data source file after the indexing process completes.

- 2 Log on to the Enforce Server administration console.
- Navigate to the screen Manage > Data Profiles > Indexed Documents > Configure Document Profile.
- Select the file from the Reference Archive on Enforce Server pull-down menu.

Note: A document source currently referenced by another Indexed Document **Profile** does not appear in the list.

5 Specify one or more file name or file size filters (optional).

See "Filtering documents by file name" on page 489.

- Select one of the indexing options (optional). See "Scheduling document profile indexing" on page 492.
- 7 Click **Save** to save the document profile.

Requirements to use the option Reference Archive on Enforce Server Table 20-15

Requirement	Description
ZIP file only	The document archive must be a ZIP file; no other encapsulation formats are supported for this option.
2 GB or less	2 GB is the maximum file size of the IDM profile. Consider using a third-party solution (such as Secure FTP), to copy the ZIP file securely to the Enforce Server.
	See "About the document data source" on page 466.
Subfiles not archived	Make sure the subfiles are proper and not encapsulated in an archive (other than the top-level profile archive).
	See "Do not compress files in the document source" on page 500.
	See "Do not index empty documents" on page 501.
UTF-8 file names only	Do not use this method if any of the names of the files you are indexing contain non-ASCII file names.
	Use either of the following options instead:
	<ul> <li>Use Local Path on Enforce Server         See "Using local path on Enforce Server" on page 485.</li> <li>Use Remote SMB Share         See "Using the remote SMB share option to index file shares" on page 486.</li> </ul>

#### Using local path on Enforce Server

The Use Local Path on Enforce Server method lets you index individual files that are local to the Enforce Server. With this method the files to be indexed cannot be archived in a ZIP file. The system deletes the documents after the indexing process completes.

See "Creating and modifying Indexed Document Profiles" on page 479.

To use the Use Local Path on Enforce Server method of making the document source available to the Enforce Server for indexing, you enter the local path to the directory that contains the documents to index. For example, if you copied the files to the file system at directory C:\Documents, you would enter C:\Documents in the field for the Use Local Path on Enforce Server option. You must specify the exact path, not a relative path. Do not include the actual file names in the path.

Note: If the files you index include a file that is more than 2 GB in size, the system will index all the files except the 2 GB file. This only applies to the Use Local Path on Enforce Server option. It does not apply to the Reference Archive on Enforce Server option.

#### Using the remote SMB share option to index file shares

The Use Remote SMB Share method lets you index documents remotely using the Common Internet File System (CIFS) protocol. To use this method of making the document source available to the Enforce Server, you enter the Universal Naming Convention (UNC) path for the Server Message Block (SMB) share that contains the documents to index

See "About indexing remote documents" on page 467.

See "To index remote documents on file shares using CIFS" on page 486. provides the steps for using CIFS to index remote documents.

Note: Symantec Data Loss Prevention does not delete documents after indexing when you use the **Use Remote SMB Share** option.

#### To index remote documents on file shares using CIFS

- Log on to the Enforce Server administration console.
- 2 Navigate to the screen Manage > Data Profiles > Indexed Documents > **Configure Document Profile.**
- 3 Select the option Use Remote SMB Share.
- 4 Enter the **UNC Path** for the SMB share that contains the documents to index.
  - A UNC path consists of a server name, a share name, and an optional file path, for example: \\server\\share\\file path.
- 5 Enter a valid user name and password for the share, and then re-enter the password. The user you specify must have general access to the shared drive and read permissions for the constituent files.
  - Optionally, you can **Use Saved Credentials**, in which case the credentials are available from the pull-down menu.
  - See "About the credential store" on page 131.
- Complete the configuration of the **Indexed Document Profile**.
  - See "Creating and modifying Indexed Document Profiles" on page 479.

#### Using the remote SMB share option to index SharePoint documents

To remotely index files on SharePoint, you expose the remote file share using WebDAV. Once you have enabled WebDAV for SharePoint, you use the Use **Remote SMB Share** option and enter the UNC path to index the remote documents. Symantec Data Loss Prevention supports remote IDM indexing using WebDAV for SharePoint 2007 and SharePoint 2010 instances.

See "About indexing remote documents" on page 467.

Table 20-16 provides the procedure for remotely indexing SharePoint documents using WebDAV

Table 20-16 Remote IDM Indexing of SharePoint documents

Step	Task	Description
1	Enable WebDAV for SharePoint.	See "Enabling WebDAV for Microsoft IIS" on page 488.
2	Start the WebClient service.	From the computer where the Enforce Server is installed, start the <b>WebClient</b> service using the "Services" console. If this service is "disabled," right-click it and select <b>Properties</b> . <b>Enable</b> the service, set it to <b>Manual</b> , then <b>Start</b> it. <b>Note:</b> You must have administrative privileges to enable this service.
3	Access the SharePoint instance.	From the computer where your Enforce Server is installed, access SharePoint using your browser and the following address format:  http:// <server_name>:port  For example: http://protect-x64:80</server_name>
4	Log on to SharePoint as an authorized user.	You do not need to have SharePoint administrative privileges.
5	Locate the documents to scan.	In SharePoint, navigate to the documents you want to scan. Often SharePoint documents are stored at the <b>Home &gt; Shared Documents</b> screen. Your documents may be stored in a different location.
6	Find the UNC path for the documents.	In SharePoint for the documents you want to scan, select the option <b>Library</b> > <b>Open with Explorer</b> . Windows Explorer should open a window and display the documents. Look in the <b>Address</b> field for the path to the documents. This address is the UNC path you need to scan the documents remotely. For example: \\protect-x64\Shared Documents. Copy this path to the Clipboard or a text file.
7	Create the IDM Index.	See "Creating and modifying Indexed Document Profiles" on page 479.

Step	Task	Description
8	Configure the SharePoint remote indexing source.	To configure the remote indexing source:  For the Document Source field, select the Use Remote SMB Share option.  For the UNC Path, paste (or enter) the address you copied from the previous step. For example: \\protect-x64\\Shared Documents.  For the User Credentials, enter your SharePoint user name and password, or select the same from the Saved Credentials drop-down list.  Select the option Submit Indexing on Save and click Save.
9	Verify success.	At the <b>Manage &gt; Data Profiles &gt; Indexed Documents</b> screen you should see that the index was successfully created. Check the "Status" and the number of documents indexed. If the index was successfully created you can now use it to create IDM policies.  See "Troubleshooting SharePoint document indexing" on page 489.

Table 20-16 Remote IDM Indexing of SharePoint documents (continued)

#### **Enabling WebDAV for Microsoft IIS**

There are various methods for enabling WebDAV for IIS. The following steps provide one approach, in this case for a Windows Server 2008 R2. This approach is provided as an example only. Your approach and environment may differ.

Microsoft IIS deployments that host SharePoint instances can be enabled to accept WebDAV connections from web clients.

See "Using the remote SMB share option to index SharePoint documents" on page 487.

#### Enable WebDAV for SharePoint

- 1 Log on to the SharePoint system where you want to enable WebDAV.
- 2 Open the Internet Information Services (IIS) Manager console.
- 3 Select the server name in the IIS tree.
- 4 Expand the tree, click the Web Sites folder and expand it.
- 5 Select the SharePoint instance from the list.
- 6 Right-click the SharePoint instance and select **New > Virtual Directory**.
- 7 The Virtual Directory Creation Wizard will appear. Click Next.
- 8 Enter a name in the Alias field (such as "WebDAV") and click Next.
- Enter a directory path in the **Web Site Content Directory** field. It can be any 9 directory path as long as it exists. Click Next.

- 10 Select Read access and click Next.
- 11 Click Finish.
- 12 Right-click the virtual directory that you created and select **Properties**.
- 13 In the Virtual Directory tab, select the option "A redirection to a URL" and click **Create**. The alias name is populated in the **Application Name** field.
- 14 Enter the SharePoint site URL in the "Redirect to" field and click **OK**. WebDAV is now enabled for this SharePoint instance.

#### **Troubleshooting SharePoint document indexing**

If you cannot connect the Enforce Server computer to the SharePoint Server computer after enabling WebDAV, make sure that you have started the WebClient service on the Enforce Server computer. You must start this service and test the WebDAV connection before you configure IDM indexing.

See "Using the remote SMB share option to index SharePoint documents" on page 487.

If you plan to re-index SharePoint documents periodically as they are updated, it may be useful to map the remote network resource to the local computer where the Enforce Server is installed. You can use the "net use" MS-DOS command to map SharePoint using the UNC path. For example:

- net use This command without parameters retrieves and displays a list of network connections.
- net use s: \\sharepoint server\Shared Documents This command assigns (maps) the SharePoint server to the local "S" drive.
- net use \* \\sharepoint server\Shared Documents This command assigns (maps) the SharePoint server to the next available letter drive.
- net use s: /delete This command removes the network mapping to the specified drive.

#### Filtering documents by file name

When you configure an Indexed Document Profile, you have the option of using filters to include or exclude documents in your data source from being indexed. There are two types of file name filters: File Name Include Filters and File Name Exclude Filters. Symantec recommends that if you choose to use file name filters you select either inclusion filters or exclusion filters, but not both.

See "Filter documents from indexing to reduce false positives" on page 504.

Table 20-17 describes the differences between the include and exclude filters for file names.

File name filters distinguished Table 20-17

Filter	Description
File Name Include Filters	If the File Name Include Filters field is empty, matching is performed on all documents in the document profile. If you enter anything in the File Name Include Filters field, it is treated as an inclusion filter. In this case the document is indexed only if it matches the filter you specify.
	For example, if you enter $*$ . docx in the <b>File Name Include Filters</b> field, the system will index only the $*$ . docx files in the document source.
File Name Exclude Filters	The Exclude Filters field lets you specify the documents to exclude in the matching process.
	If you leave the Exclude Filters field empty, the system performs matching on all documents in the ZIP file or file share. If you enter any values in the field, the system scans only those documents that do not match the filter.

The system treats forward slashes (/) and backslashes (\) as equivalent. The system ignores whitespace at the beginning or end of the pattern. File name filtering does not support escape characters, so you cannot match on literal question marks, commas, or asterisks.

Table 20-18 describes the syntax accepted by the File Name Filters feature. The syntax for the Include and Exclude filters is the same.

Table 20-18 File name filtering syntax

Operator	Description
Asterisk (*)	Represents any number of characters.
Question mark (?)	Represents a single character.
Comma (,) and newline	Represents a logical OR.

Table 20-19 provides sample filters and descriptions of behavior if you enter them in the File Name Include Filters field:

Filter string	Description
*.txt,*.docx	The system indexes only .txt and .docx files in the ZIP file or file share, ignoring everything else.
?????.docx	The system indexes files with the .docx extension and files with five-character names, such as hello.docx and stats.docx, but not good.docx or marketing.docx.
*/documentation/*,*/specs/*	The system indexes only files in two subdirectories below the root directory, one called "documentation" and the other called "specs."
Example with wildcards and sub-directories:	IDM indexing fails or ignores the filter setting if the File Name Includes / Excludes filter string starts with an alphanumeric character and includes a wildcard, for
*\scan_dir\l*.txt	example: l*.txt. The workaround is to configure the include/exclude filter with the filter string as indicated in this example, that is, *\scan_dir\l*.txt.
	For example, the filter 1*.txt does not work for a file path \\dlp.symantec.com\scan_dir\lincoln-LyceumAddress.txt. However, if the filter is configured as *\scan_dir\l*.txt, the indexer will acknowledge the filter and index the file.

Table 20-19 File name filter examples

#### Filtering documents by file size

Filters let you specify documents to include or exclude from indexing. The types of filters include File Name Include Filters, File Name Exclude Filters, and File Size Filters. You use file size filters to exclude files from the matching process based on their size. Any files that match the size filters are ignored.

See "Filtering documents by file name" on page 489.

In the Size Filters fields, specify any restrictions on the size of files the system should index. In general you should use only one type of file size filter.

See "Filter documents from indexing to reduce false positives" on page 504.

Table 20-20 describes the file size filter options.

Table 20 20 The size little configuration options		
Filter	Description	
Ignore Files Smaller Than	To exclude files smaller than a particular size:  • Enter a number in the field for Ignore Files Smaller Than.	
	■ Select the appropriate unit of measure Bytes, KB (kilobytes), or MB (megabytes) from the drop-down list.	
	For example, to prevent indexing of files smaller than one kilobyte (1 KB), enter ${\tt 1}$ in the field and select ${\tt KB}$ from the corresponding drop-down list.	
Ignore Files Larger Than	To exclude files larger than a particular size:	
	<ul> <li>Enter a number in the field for Ignore Files Larger Than.</li> <li>Select the appropriate unit of measure (Bytes, KB, or MB) from the drop-down list.</li> </ul>	
	For example, to prevent indexing of files larger than two megabytes (2 MB), enter 2 in the field and select MB from the corresponding drop-down list.	

Table 20-20 File size filter configuration options

#### Scheduling document profile indexing

When you configure a document profile, select Submit Indexing Job on Save to index the document profile as soon as you save it. Alternatively, you can set up a schedule for indexing the document source.

To schedule document indexing, select Submit Indexing Job on Schedule and select a schedule from the drop-down list as described in Table 20-21.

Note: The Enforce Server can index only one document profile at a time. If one indexing process is scheduled to start while another indexing process is running, the new process does not begin until the first process completes.

Options for scheduling Document Profile indexing Table 20-21

Parameter	Description	
Index Once	<b>On</b> – Enter the date to index the document profile in the format MM/DD/YY. You can also click the date widget and select a date.	
	At – Select the hour to start indexing.	
Index Daily	At – Select the hour to start indexing.	
	<b>Until</b> – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.	

Parameter	Description
Index Weekly	Day of the week – Select the day(s) to index the document.
	At – Select the hour to start indexing.
	<b>Until</b> – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.
Index Monthly	Day – Enter the number of the day of each month you want the indexing to occur. The number must be 1 through 28.
	At – Select the hour to start indexing.
	<b>Until</b> – Select this check box to specify a date in the format MM/DD/YY when the indexing should stop. You can also click the date widget and select a date.

Table 20-21 Options for scheduling Document Profile indexing (continued)

## Changing the default indexer properties

The server index contains the MD5 fingerprint of each file that has been indexed. either raw binary or 100% extracted content if the file can be cracked, and hashes of discrete passages of content.

See "Using IDM to detect exact and partial file contents" on page 471.

The size of the passages depends on the "k" and "t" settings in the indexer properties file (\SymantecDLP\Protect\config\indexer.properties). Generally, there is no need to change the default settings. When you lower the default minimum, the Enforce Server creates hashes out of smaller sections of the documents it indexes. The lower the default minimum, the greater the number of hashes that the Enforce Server requires for your documents. The greater number of hashes increases index size as well as computational load during detection.

The default settings apply to the Whitelisted.txt file as well. If the amount of content you need to whitelist is less than the minimum amount required for partial matching, you can adjust the default minimum setting.

#### To change the default minimum for whitelisted text

- 1 On the Symantec Data Loss Prevention host, navigate to directory \SymantecDLP\Protect\config on Windows, or /opt/SymantecDLP/Protect/config on Linux.
- 2 Use a text editor to open file Indexer.properties
- Locate the parameter Guarantee threshold t:

```
# Guarantee threshold t
com.vontu.profiles.documents.t=130
```

Change the numerical portion of the parameter value to reflect the wanted minimum number of characters that are allowed in Whitelisted.txt.

For example, to change the minimum to 80 characters, modify the value to look like the following:

```
# Guarantee threshold t
com.vontu.profiles.documents.t=80
```

#### Save the file. 5

In addition, the maximum size that can be processed for content extraction at run-time is 30 MB and is set by the max bin match size=30000000 parameter. Increasing this number is not recommended.

#### Using agent IDM after upgrade to version 12.5

For upgrades to Symantec Data Loss Prevention version 12.5, exact match IDM is disabled and two-tier detection is the default setting. This means that if you take no action after upgrade your IDM policies will continue to use two-tier detection for endpoint deployments.

To use exact match IDM on the endpoint after upgrade, you must enable it and reindex the document data source. Reindexing is required even if the data source is unchanged so that the endpoint indexes are generated.

Table 20-22 describes the workflow for implementing agent IDM for customers upgrading to version 12.5.

Table 20-22 Using agent IDM after upgrade to version 12.5

Step	Action	Description
1	Upgrade Data Loss Prevention to version 12.5.	You must upgrade the Enforce Server and Endpoint Servers to version 12.5.  Refer to the Symantec Data Loss Prevention Upgrade Guide.
		Trees to the dynamics but 2000 i revention opgrade duide.
2	Reindex existing IDM profiles.	To use agent IDM you must update each Indexed Document Profiles so that the endpoint index is generated.
		See "Reindex IDM profiles after major upgrade" on page 500.
		See "Creating and modifying Indexed Document Profiles" on page 479.

Step	Action	Description
3	Upgrade DLP Agent to version 12.5.	To use exact match IDM on the endpoint you must upgrade the DLP Agent to version 12.5.
		Refer to the Symantec Data Loss Prevention Upgrade Guide.
		<b>Note:</b> During the upgrade process, you may have a period where you have both 12.5 DLP Agents and 12.0.x and earlier DLP Agents. If this is the case, consider segregating 12.5 DLP Agents from 12.0.x and earlier DLP Agents using different Endpoint Servers so that you can use two-tier detection for the former and agent IDM for the latter.
4	Enable agent IDM.	Agent IDM is disabled for an Endpoint Server upgraded to version 12.5.  To use agent IDM you must enable it.  See "Enabling agent IDM" on page 495.
5	Apply the configuration to DLP Agents.	Apply the agent configuration settings to DLP Agents.
	DLI Agents.	See "Applying agent configurations to an agent group" on page 1441.
		Once the configuration is applied, the DLP Agent will download the endpoint index from the Endpoint Server the next time the agent connects.
5	Test IDM policies.	It is recommended that you test your IDM policies after you have upgraded the system and updated the IDM profiles.

Table 20-22 Using agent IDM after upgrade to version 12.5 (continued)

## **Enabling agent IDM**

You enable exact match IDM on the endpoint by setting the advanced agent configuration parameter Detection. TWO TIER IDM ENABLED. str to OFF. Once two-tier detection is OFF, the DLP Agent performs exact file and exact file contents matching, assuming you have generated the endpoint index.

See "Creating and modifying Indexed Document Profiles" on page 479.

For new installations, exact match IDM on the endpoint is the default setting for the default endpoint agent configuration (TWO TIER IDM ENABLED = OFF); you do not need to enable it.

For upgraded systems, exact match IDM on the endpoint is disabled (TWO TIER IDM ENABLED = ON) so that there is no change in functionality for existing IDM policies deployed to the endpoint. If you want to use exact match IDM on the endpoint after upgrade, you need to turn off two-tier detection and reindex each document data source.

See "Using agent IDM after upgrade to version 12.5" on page 494.

See "To turn two-tier detection on or off" on page 496, provides steps for enabling and disabling exact match IDM on the endpoint.

#### To turn two-tier detection on or off

- Log on to the Enforce Server administration console.
- 2 Navigate to **System > Agents > Agent Configuration**.
- 3 Select the applicable agent configuration.
- 4 Select the Advanced Agent Settings tab.
- 5 Locate the Detection. TWO TIER IDM ENABLED. str parameter.
- Change the value to either "ON" or "OFF" (case insensitive) depending on your requirements.
  - See Table 20-23 on page 496.
- 7 Click **Save** at the top of the page to save the changes.
- Apply the agent configuration to the agent group or groups. See "Applying agent configurations to an agent group" on page 1441.

Table 20-23 Advanced agent settings for exact match IDM on the endpoint

Advance Agent Setting parameter	Value	Default	Detection engine	Matching type
Detection.TWO_TIER_IDM_ENABLED.str			DLP Agent	Exact file
		installation		Exact file contents
	ON	System upgrade to 12.5	Endpoint Server	Exact file
				Exact file contents
				Partial file contents

#### Estimating endpoint memory use for agent IDM

The endpoint index is small because it only contains MD5 hashes of each file or exact file contents; it does not contain hashes for partial file contents matching. Nonetheless, you should be aware of estimated endpoint memory requirements for DLP Agents that will perform exact IDM locally.

See "About the server and agent index files" on page 467.

The following tables provide some guidance around memory usage on the endpoint for an IDM index deployed there.

Number of files indexed	Total Memory (KB)	Memory per file (bytes)
1503	172	117
3154	436	141
5787	584	103
10000	956	97
17621	1820	105

Table 20-24 DLP Agent for Windows 32-bit

When the same number of files are indexed and the endpoint index is deployed to a 64-bit DLP Agent for Windows, there is different memory consumption on the endpoint than for 32-bit DLP Agents. This difference has to do with the way memory is used on 32-bit systems versus 64-bit systems. The memory usage on 64-bit systems is not exactly double that of 32-bit systems because of the way the index is stored.

DLP Agent for Windows 64-bit Table 20-25

Number of files indexed	Total Memory (KB)	Memory per file (bytes)
1503	244	166
3154	648	210
5787	864	152
10000	1416	144
17621	2636	153

#### Configuring the Content Matches Document Signature policy condition

The Content Matches Document Signature From matches unstructured document content based on the Indexed Document Profile. The Content Matches Document **Signature From** condition is available for detection rules and exceptions.

See "About using the Content Matches Document Signature policy condition" on page 473.

#### To configure the Content Matches Document Signature condition

1 Add an IDM condition to a policy rule or exception, or modify an existing one.

See "Configuring policies" on page 326.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

2 Configure the IDM condition parameters.

See Table 20-26 on page 498.

3 Save the policy configuration.

Table 20-26 Content Matches Document Signature condition parameters

Action	Description	
Set the Minimum	Select an option from the drop-down list.	
Document Exposure.	Choose <b>Exact</b> to match document contents exactly.	
	Choose a percentage between 10% and 90% to match document contents partially.	
Configure Match	Select how you want to count matches:	
Counting.	■ Check for existence	
	Reports a match count of 1 if there are one or more condition matches.	
	■ Count all matches	
	Reports a match count of the exact number of matches.	
	See "Configuring match counting" on page 334.	
Select the components to	Select one of the available message components to match on:	
Match On.	■ Body – The content of the message.	
	■ Attachments – Any files that are attached to or transferred by the message.	
	See "Selecting components to match on" on page 336.	
Configure additional conditions to Also Match.	Select this option to create a compound condition. All conditions must be met to trigger or except a match.	
	You can <b>Add</b> any available condition from the drop-down menu.	
Test and tune the policy.	See "Test and tune policies to improve match accuracy" on page 361.	
	See "Use parallel IDM rules to tune match thresholds" on page 507.	
	See "Troubleshooting policies" on page 353.	

# Best practices for using IDM

Indexed Document Matching (IDM) is designed to protect document content and images. IDM relies on an index of fingerprinted documents to perform partial and derivative text-based content matching. In addition, you can also use IDM to match indexed documents exactly based on their binary stamp, including not only text-based documents but also graphics and media files

Because of the broad range of matching supported by IDM, you should consider the best practices in this section to implement IDM policies that accurately match the data you want to protect.

Table 20-27 summarizes the IDM considerations discussed in this section, with links to individual topics for each.

IDM policy best practices Table 20-27

Consideration	Description	
Reindex IDM profiles after upgrade.	See "Reindex IDM profiles after major upgrade" on page 500.	
Do not compress documents whose content you want to fingerprint.	See "Do not compress files in the document source" on page 500.	
Do not use IDM solely to protect binary files.	See "Avoid using IDM solely for binary files" on page 501.	
Do not index text-based documents without content.	See "Do not index empty documents" on page 501.	
Use exact matching IDM on the endpoint instead of two-tier detection wherever possible.	See "Prefer exact match over two-tier detection on the endpoint" on page 502.	
Be aware of the limitations of exact matching.	See "Understand limitations of exact matching" on page 502.	
Use whitelisting to exclude partial file contents from matching and reduce false positives.	See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.	
Filter non-critical documents from indexing to reduce false positives.	See "Filter documents from indexing to reduce false positives" on page 504.	
Use IDM as an exception to exclude files from exact matching.	See "Distinguish IDM exceptions from whitelisting and filtering" on page 505.	
Create more than one profile to index more than 2 GB of documents.	See "Create separate profiles to index large document sources" on page 505.	
Use remote indexing for large document sets.	See "Use WebDAV or CIFS to index remote document data sources" on page 506.	

Consideration	Description	
Use scheduled indexing to automate profile updates.	See "Use scheduled indexing to keep profiles up to date" on page 506.	
Use multiple IDM rules in parallel to establish and tune match thresholds.	See "Use parallel IDM rules to tune match thresholds" on page 507.	
Use VML with exact match agent IDM on the endpoint.	See "Use agent IDM with VML for partial match validation" on page 507.	

**Table 20-27** IDM policy best practices (continued)

#### Reindex IDM profiles after major upgrade

It is recommended that you update each Indexed Document Matching profile by reindexing each associated data source after performing a major upgrade of Symantec Data Loss Prevention.

If you have upgraded to Symantec Data Loss Prevention version 12.5 and you want to use exact match IDM on the endpoint for existing IDM policies, you must reindex the data source for each Indexed Document Profile so that each endpoint index is generated and deployed to DLP Agents.

If you have upgraded to Data Loss Prevention 12.5 and you are not using agent IDM, you are not required to reindex your data sources, but doing so is recommended.

See "Using agent IDM after upgrade to version 12.5" on page 494.

See "Enabling agent IDM" on page 495.

#### Do not compress files in the document source

For file formats whose content can be cracked, the server indexing process opens the document, extracts the text-based content, and fingerprints the data in full and in part (sections). However, the indexing process cannot recursively inspect document archives that are contained in the document set. If a document whose file contents you want to index is compressed in an archive file (such as ZIP, RAR, or TAR) within the document data source, the system cannot crack the file and index its content. In this case, the system will only take an MD5 hash of the binary file signature. The embedded file is considered for exact file matches only, like image files and other unsupported file formats.

This behavior is specific to the design-time indexing process only. At run-time the detection server does recursively inspect document archives and extract the text

of files contained in those archives. But, to be able to evaluate such content, the IDM index must have been able to index all content files.

The best practice is not to include any files whose content you want to index in a document archive. The lone exception is the document archive ZIP file that you upload or copy to the Enforce Server that contains the entire document set. All files in that container file must be uncompressed. If the Document Archive uploaded to the Enforce Server for indexing contains one or more embedded archive files (such as a ZIP), the system performs an exact binary match on any file contained in the embedded archive file

See "Creating and modifying Indexed Document Profiles" on page 479.

#### Avoid using IDM solely for binary files

Although IDM can protect any type of file, unless you must protect the exact file, the general recommendation is that if you only need to protect binary files, consider using the **File Type Match** condition instead of IDM. There is less overhead in creating file-type matching policies, and the **File Type Match** condition executes locally on the endpoint.

See "Use compound file property rules to protect design and multimedia files" on page 618.

For example, if you want to detect CAD files that contain IP diagrams, you could index these files and apply IDM rules to detect them. Alternatively, you could create a policy that contains a file type rule that detects on the CAD file format plus a file size rule that specifies a threshold size. The file property approach is preferred in this scenario because all you really care about is protecting large CAD files potentially leaving the company. You do not need to gather and index these files for IDM if you can simply create rules that will detect on the file type and the file size.

## Do not index empty documents

You should be careful about the documents you index. In particular, avoid indexing blank or empty documents.

For example, indexing a PPTX file containing only photographs or other graphical content but no textual content will match other blank PPTX files exactly and produce false positives. Is this case, even though a PPTX file contains no user-entered text, the file does contain header and footer placeholder text that the system extracts as file contents. Because the amount of text extracted and normalized is more than 30 non-whitespace characters, the system treats the file as not binary and creates an MD5 hash of 100% of the file contents. As a result, all other blank PPTX files

will produce exact file contents matches because the resulting MD5 of the extracted content is the same.

Note: This behavior has not been observed with XLSX files; that is, false positives do not get created if the blank files are different.

See "Using IDM to detect exact and partial file contents" on page 471.

## Prefer exact match over two-tier detection on the endpoint

If you are deploying IDM polices to the endpoint, in general agent IDM is recommended over two-tier IDM. The main advantage of agent IDM over two-tier IDM is that matching is faster because it is done locally by the agent instead of remotely by the server. In addition, agent IDM lets you use response rules directly on the endpoint. The disadvantage of agent IDM is that it does not support partial file contents matching.

See "Types of IDM detection" on page 464.

To overcome the limitation of the lack of support for partial file contents matching, consider using agent IDM with VML rules on the endpoint.

See "Use agent IDM with VML for partial match validation" on page 507.

## Understand limitations of exact matching

Exact match means just that: inbound data must match the MD5 fingerprint of either a binary file signature or 100% of extracted and normalized file contents.

See "Supported forms of matching for IDM" on page 463.

Consider the following when implementing exact match IDM:

- You cannot use whitelisting to exclude content from exact matching on the endpoint. When the system generates the endpoint index file, it ignores the whitelisted.txt file. Whitelisting only applies to server-based partial file contents matching.
- If exact match IDM on the endpoint is enabled, documents will be matched exactly by the DLP Agent regardless of the match percentage level you choose in the IDM rule.
- For binary files coming into the detection engine for exact file matching, as an optimization the system checks the byte size of the file before computing the run-time MD5 for comparison against the index. If the file byte sizes do not match there is no comparison of the MD5 hashes.

- For content extracted from a text-based file coming into the detection engine for exact file contents matching, file size is not checked. If text can be extracted the system always computes and compares the MD5 for matching.
- File type is never checked for exact file or exact file contents matching.
- Some file formats change the byte size of a file if the file is opened by the native application and then resaved without changes, resulting in the file not matching exactly. For example, if you open a file such as a JPEG image with Windows Picture and Fax Viewer and resave the file without making changes, the binary size of the file is nonetheless changed, resulting in no exact match.
- For some applications the Windows Print operation may alter the file data such that extracted file contents will not match exactly. Known file types that are affected by this include Microsoft Office documents.

Table 1 lists some known limitations with exact content matching. This list is not exhaustive and there may be other file formats that change on resave.

File type	Application	Result on resave
dwg	AutoCAD 2012	Does not match
jpeg	Windows Picture and Fax Viewer	Does not match
doc	Microsoft Office Word 2007	Does not match
xls	Microsoft Excel 2007	Does not match
ppt	Microsoft Presentation 2007	Does not match
pdf	Adobe Acrobat 9 Pro	Does not match
docx	Microsoft Office Word 2007	Match
xlsx	Microsoft Excel 2007	Match

 Table 1
 Limitations of exact file content matching

# Use whitelisting to exclude non-sensitive content from partial matching

Microsoft Presentation 2007

pptx

Whitelisting is designed to let you exclude partial file contents from matching. You use whitelisting to exclude headers, footers, and boilerplate content from partial matching and reduce false positives. Information contained in document headers and footers is likely to cause false positives. Likewise boilerplate text, such as

Match

standard language and non-proprietary corporate content that is often repeated across confidential documents can cause false positives.

Ideally, you should remove headers and footers from documents before you index them. However, this may not be feasible, especially if you have a large document set. As a best practice, you should whitelist header, footer, and boilerplate content so that this text is excluded when the server index is generated. If you use whitelisting, generally you can lower the **Minimum Document Exposure** setting in the policy without increasing false positives because more of the content indexed is confidential data, instead of common, repeated content.

**Note:** Whitelisting does not apply to exact file or exact file contents matching.

See "About whitelisting partial file contents" on page 474.

See "Whitelisting file contents to exclude from partial matching" on page 476.

#### Filter documents from indexing to reduce false positives

When you configure an Indexed Document Profile, you have the option of using filters to include or exclude documents in your data source for indexing. There are two types of filters: file name and file size.

See "Creating and modifying Indexed Document Profiles" on page 479.

You use filtering to filter non-critical documents from indexing and ensure that your index is protecting only confidential files and file contents. Filtering helps reduce false positives and decrease the size of the IDM index.

See "Do not index empty documents" on page 501.

The best practice is to use either an exclusion filter or an inclusion filter for each filter type, but not both. For example, you may not need to index all of the files you include in a document archive or expose to the system by file share. In this case, you can enumerate the files you want to include (inclusion filter) or list the file types you want to exclude from indexing (exclusion filter), but you should not use both. You can also use file size filters to set a threshold for the file size to include or exclude in the index.

See "Filtering documents by file name" on page 489.

See "Filtering documents by file size" on page 491.

## Distinguish IDM exceptions from whitelisting and filtering

Whitelisting lets you exclude partial file contents from matching. Filtering lets you exclude specific documents from the indexing process. IDM exceptions, on the other hand, let you except indexed files from exact matching at run-time.

You use the IDM condition as policy exception to exclude files from detection. To be excepted from matching, an inbound file must be an exact match with a file in the IDM index. You cannot use IDM exceptions to exclude content from matching. To exclude content, you must whitelist it.

**Note:** Whitelisting is not available for exact file or file contents matching; it is only available for partial content matching.

**Table 20-29** Whitelisting, filters, and exceptions distinguished

IDM Configuration	Use
Exception	Except exact file from matching
	See "About using IDM for policy exceptions" on page 474.
	As an example, the CAN-SPAM Act policy template uses an IDM exception.
	See "CAN-SPAM Act policy template" on page 805.
Whitelisting	Except file contents from matching
	See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.
Filtering	Include or exclude files from being indexed
	See "Filter documents from indexing to reduce false positives" on page 504.

## Create separate profiles to index large document sources

IDM detection is based on an Indexed Document Profile. The maximum size of the source documents that you can index for a single IDM profile is 2 GB. This maximum size limit is based on the overall size of the documents in their natural, uncompressed state. Depending on the size of the actual source files and their extracted text size, this translates into approximately 300,000 to 400,000 files. In addition, the 2 GB maximum size may be affected by any hardware limitations imposed by the host machine where the Enforce Server is installed.

See "About the document data source" on page 466.

If you need to index a large number of files more than 2 GB in total size when uncompressed, the best practice is to organize the documents into separate ZIP

files or share directories. You then create a separate Indexed Document Profile for each individual document set. You can then define separate rules that reference each index and add the rules one or more policies.

### Use WebDAV or CIFS to index remote document data sources

For smaller document sets (50 MB or less), you can upload the files to the Enforce Server. For larger document sets, consider using FTP Secure to upload the files to the Enforce Server.

Alternatively, you can use the remote IDM indexing feature to remotely index documents that are stored on a file share that supports the CIFS protocol, or on a web server that supports the WebDAV protocol, such as Microsoft SharePoint or OpenText Livelink

See "About indexing remote documents" on page 467.

## Use scheduled indexing to keep profiles up to date

You can use index scheduling to keep your IDM profiles up to date. The initial index scans all the documents to be indexed. Any subsequent index only scans the differences between the two. You should schedule indexing outside of normal business hours to reduce any potential affect on the system.

See "Scheduling document profile indexing" on page 492.

Before you set up an indexing schedule, consider the following recommendations:

- If you update your document sources occasionally (for example, less than once a month), there is no need to create a schedule. Index the document each time you update it.
- Schedule indexing for times of minimal system use. Indexing affects performance throughout the Symantec Data Loss Prevention system, and large documents can take time to index.
- Index a document as soon as you add or modify the corresponding document profile, and re-index the document whenever you update it. For example, consider a situation where every Wednesday at 2:00 A.M. you update a document. In this case scheduling the index process to run every Wednesday at 3:00 A.M. is optimal. Scheduling document indexing daily is not recommended because that is too frequent and can degrade server performance.
- Monitor results and modify your indexing schedule accordingly. If performance is good and you want more timely updates, schedule more frequent document updates and indexing.

Symantec Data Loss Prevention performs incremental indexing. When a previously indexed share or directory is indexed again, only the files that have changed or been added are indexed. Any files that are no longer in the archive are deleted during this indexing. So a reindexing operation can run significantly faster than the initial indexing operation.

## Use parallel IDM rules to tune match thresholds

The primary use case for IDM policies is to detect unstructured document content based on a percentage match requirement called the Minimum Document Exposure. This value is a configurable parameter that specifies the minimum percentage of content in the message that must match the IDM index to produce a match. The IDM policy default is "Exact," which means that, for text-based documents, 100% of the content of the message must match the fingerprint to create an incident. A Minimum Document Exposure setting of 10% means that, on average, one page of a 10 page document must match the IDM index to create an incident

A document might contain much more content, but Symantec Data Loss Prevention protects only the content that is indexed as part of a document profile. For example, consider a situation where you index a one-page document, and that one-page document is included as part of a 100-page document. The 100-page document is considered a 100 percent match because its content matches the one-page document exactly. In addition, the matched document does not have to be of the same file type or format as the indexed document. For example, if you index a Word document as part of a document profile, and its contents are pasted into the body of an email message or used to create a PDF, the engine considers it a match

A rule-of-thumb for setting the Minimum Document Exposure setting is 60%. Minimum Document Exposures set to less than 50% typically create many false positives. Starting with rate of 60% should give you enough information to determine whether you should go to a higher or lower match percentage without creating excessive false positives

As an alternative, consider taking a tiered approach to establishing Minimum Document Exposure settings. For example, you can create multiple IDM rules, each with a different threshold percentage, such as 80% for documents with a high match percentage, 50% for documents with a medium match percentage, and 10% with a low match percentage. Using this approach will help you filter out false positives and help you establish an accurate Minimum Document Exposure setting for each IDM index you deploy as part of your policies.

## Use agent IDM with VML for partial match validation

The DLP Agent does not support partial file contents matching for IDM. If exact match IDM on the endpoint is enabled, the DLP Agent only matches exact files and

exact file contents. If two-tier detection for IDM is enabled, the DLP Agent sends message contents to the server for matching. If the endpoint is offline, the DLP Agent cannot send the message contents to the server for matching.

If you want to match partial file contents locally on the endpoint, consider creating a compound policy that includes IDM and VML rules. VML indexes run locally on the endpoint; they do not require two-tier detection. Using a VML rule with the IDM you can detect similar document content when the endpoint is offline. To do this you take a subset of the IDM documents you have indexed and create a VML index that is deployed to the endpoint. In a single policy you create separate IDM and VML rules so that their logical connection is an OR. With this policy configuration, if the file contents do not match exactly, they can still be matched similarly according to the VML rule configuration.

In addition, VML may be viable as an exception for IDM rules. For example, where an IDM policy is a consistent source of false positives, you can implement VML as an exception to the IDM rule. For example, a sales report may consistently produce false positives for explicit pre-release data that is not sensitive. VML may work well here because you can train against the content that causes the false positives and create an exception to ignore those features. Refer to the VML documentation for details.

# Detecting content using Vector Machine Learning (VML)

This chapter includes the following topics:

- Introducing Vector Machine Learning (VML)
- Configuring VML profiles and policy conditions
- Best practices for using VML

# Introducing Vector Machine Learning (VML)

Vector Machine Learning (VML) protects unstructured data by performing statistical analysis to determine if content is similar to example content you train against.

Unlike other detection technologies, with VML you do not have to locate and fingerprint all of the data you want to protect, nor do you have to describe it and risk potential inaccuracies. With VML you train the system to learn the type of content you want to protect based on example documents you provide.

VML detection is based on a VML profile. You create a VML profile by uploading a representative amount of content from a specific category of data. The system scans the content, extracts the features, and creates a statistical model based on the frequency of keywords in the example documents. At runtime the system applies the model to analyze and detect content that has features that are statistically similar to the profile.

VML simplifies the detection of unstructured, text-based content while offering the potential for high accuracy. The key to implementing VML is the example content you train the system against. You must be careful to select documents that are very

representative of the type of content you want to protect. And, you must select good examples of content you want to ignore that are closely related to the content you want to protect.

See "Configuring VML profiles and policy conditions" on page 513.

## About the Vector Machine Learning Profile

The Vector Machine Learning Profile is the data profile that you define for implementing VML policies.

For example, you might create a VML profile to protect your source code. In this case you train the system using positive example documents (proprietary code that you want to protect) and negative example documents (open source code that you do not care to protect). A VML policy references the VML profile to analyze message data and recognize content that is similar to the positive features. The VML profile can be tuned, and it can be easily updated by adding or removing documents to or from the training sets.

See "Data Profiles" on page 291.

See "Creating new VML profiles" on page 515.

## About the content you train

Collecting the documents for training is the most important step in the Vector Machine Learning process. Vector Machine Learning is only as accurate as the example content you train against.

See "Configuring VML profiles and policy conditions" on page 513.

A VML profile is based on a category of content representing a specific business use case. A category of content comprises two training sets: positive and negative.

The positive training set is content you want to protect. More specific categorization results in better accuracy. For example, "Customer Purchase Orders" is better than "Financial Documents" because it is more specific.

The negative training set is content you want to ignore, yet related to the positive training set. For example, if the positive training set is "Weekly Sales Reports," the negative training set might contain "Sales Press Releases."

You should collect an equal amount of positive and negative content that is primarily text-based. You do not have to collect all the content you want to protect, but you need to assemble training sets large enough to produce reliable statistics.

The recommended number of documents is 250 per training set. The minimum number of documents per training set is 50.

The following table summarizes the baseline requirements for the content you collect for VML profile training.

Table 21-1	VML training set requirements

Category of content	Type of data	Training set	Quantity	Content	Size
Single, specific business use case	Text-based (primarily)	Positive	Recommended: 250 documents Minimum: 50 documents	Content you want to protect.	30 MB per upload  No size limit per
		Negative	Approximately the same amount as the positive category.	Content you do not want to protect yet thematically related to the positive category.	

## About the base accuracy from training percentage rates

During the VML profile training process, the system extracts example document content and converts it to raw text. The system selects features (or keywords) using a proprietary algorithm and generates the VML profile. As part of the training process, the system calculates and reports base accuracy rates for false positives and false negatives. The base accuracy from training percentage rates indicate the quality of your positive and negative training sets.

While the goal is to achieve 100% accuracy (0% base false rates), obtaining this level of quality for both training sets is usually not possible. In general you should reject a training profile if either the base false positive rate or the base false negative rate is more than 5%. A relatively high base false percentage rate indicates that the training set is not well categorized. In this case you need to add documents to an underrepresented training set or remove documents from an over-represented training set, or both.

See "Managing training set documents" on page 521.

The following table describes what the base accuracy percentage rates from training mean in relation to the positive and negative training sets for a given VML profile.

**Table 21-2** Base accuracy rates from training

Accuracy rate	Description
Base False Positive Rate (%)	The percentage of the content in the negative training set that is statistically similar to the positive content.

Accuracy rate

Description

Base False Negative Rate (%)

The percentage of the content in the positive training set that is statistically similar to negative content.

**Table 21-2** Base accuracy rates from training (continued)

## About the Similarity Threshold and Similarity Score

Each VML profile has a setting called the **Similarity Threshold** which can be set from 0 to 10. This setting is used to make an adjustment for imperfect information within a training set to achieve the best accuracy possible. During detection, a message must have a Similarity Score greater than the Similarity Threshold for an incident to be generated. The Similarity Threshold is set at the profile level—not within a policy rule—because there is an ideal Similarity Threshold setting that is unique to your training set where the best accuracy rates can be achieved (both in terms of false positives and false negatives).

When a VML policy detects an incident, the system displays the **Similarity Score** in the match highlighting section of the **Incident Snapshot** in the Enforce Server administration console. The Similarity Score indicates how similar the detected content is to the VML profile. The higher the score the more statistically similar the message is to the positive example documents in your VML profile.

Consider an example where a Similarity Threshold is set to 4 and a message with a Similarity Score of 5 is detected. In this case the system reports the match as an incident and displays the Similarity Score during match highlighting. However, if a message is detected with a Similarity Score of 3, the system does not report a match (and no incident) because the Similarity Score is below the Similarity Threshold.

The table below describes the Similarity Threshold and Similarity Score numbers.

**Table 21-3** Similarity Threshold and Similarity Score details

Similarity	Description
Similarity Threshold	The Similarity Threshold is a configurable parameter between 0 and 10 that is unique to each VML profile. The default setting is 10, which requires the most similar match between the VML profile features and the detected message content. As such, this setting is likely to produce fewer incidents. A setting of 0 produces the most number of matches, many of which are likely to be false positives.
	See "Adjusting the Similarity Threshold" on page 527.

**Table 21-3** Similarity Threshold and Similarity Score details (continued)

Similarity	Description
Similarity Score	The Similarity Score is a read-only runtime statistic between 0 and 10 reported by the system based on the detection results of a VML policy. To report an incident, the Similarity Score must be higher than the Similarity Threshold, otherwise the VML policy does not report a match.

## About using unaccepted VML profiles in policies

The system lets you create a policy that is based on a VML profile that has never been accepted. However, the VML profile is not active and is not deployed to a referenced policy until the profile is initially accepted.

See "Training VML profiles" on page 518.

Where you have a VML policy that references a never-accepted VML profile, the result of this configuration depends on the type of detection server. The table below describes the behavior:

Detection server	Description
Discover Server	Discover scanning does not begin until all policy dependencies are loaded. As such, a Discover scan based on a VML policy will not start until the referenced VML profile is accepted. In this case the system displays a message in the Discover scanning interface indicating the scan is waiting on the dependency to load.
Network and Endpoint Servers	For a simple rule, or compound rule where the conditions are ANDed, the entire rule fails because the VML condition cannot match. If this is the only rule in the policy, the policy will not work.
	For a policy where there are multiple rules that are ORed, only the VML rule fails; the other rules in the policy are evaluated.
	See "Policy detection execution" on page 308.

# Configuring VML profiles and policy conditions

Vector Machine Learning (VML) protects unstructured data by performing statistical analysis to determine if content is similar to an example set of documents you train against.

See "Introducing Vector Machine Learning (VML)" on page 509.

The following table describes the process for implementing VML.

**Table 21-4** Implementing VML

Step	Action	Description
Step 1	Collect the example documents for training the system.	Collect a representative amount of example documents containing positive content you want to protect and negative content you want to ignore.
		See "About the content you train" on page 510.
Step 2	Create a new VML profile.	Define a new VML profile based on the specific business category of data from which you have derived your positive and negative training sets.
		See "Creating new VML profiles" on page 515.
Step 3	Upload the example documents.	Upload separately to the Enforce Server the example positive and negative training sets.
		See "Uploading example documents for training" on page 516.
Step 4	Train the VML profile.	Train the system to learn the type of content you want to protect and generate the VML profile.
		See "Training VML profiles" on page 518.
Step 5	Accept or reject the trained profile.	Accept the trained profile to deploy it. Or, reject the profile, update one or both of the training sets (by adding or removing example documents), and restart the training process.
		See "About the base accuracy from training percentage rates" on page 511.
		See "Managing VML profiles" on page 522.
Step 6	Create a VML policy and test	Create a VML policy that references the VML profile.
	detection.	See "Configuring the Detect using Vector Machine Learning Profile condition" on page 525.
		Test and review incidents based on the Similarity Score.
		See "About the Similarity Threshold and Similarity Score" on page 512.
Step 7	Tune the VML profile.	Adjust the Similarity Threshold setting as necessary to optimize detection results.
		See "Adjusting the Similarity Threshold" on page 527.
Step 8	Follow VML best practices.	See "Best practices for using VML" on page 532.

## Creating new VML profiles

A VML profile contains the model that is generated from the training set contents. Once you define a VML profile, you use it to create one or more VML policies.

See "Configuring VML profiles and policy conditions" on page 513.

Note: You must have Enforce Server administrator privileges to create VML profiles.

#### To create a new VML profile

- Click New Profile from the Manage > Data Profiles > Vector Machine **Learning** screen (if you have not already done so).
- 2 Enter a **Name** for the VML profile in the **Create New Profile** dialog.

Use a logical name for the VML profile that corresponds to the category of data you want to protect.

See "About the content you train" on page 510.

3 Optionally, enter a **Description** for the VML profile.

You may want to include a description that identifies the purpose of the VML profile.

4 Click **Create** to create the new VML profile.

Or, click **Cancel** to cancel the operation.

5 Click **Manage Profile** to upload example documents.

See "Uploading example documents for training" on page 516.

## Working with the Current Profile and Temporary Workspace tabs

For any single VML profile there are two possible versions: Current and Temporary. The Current Profile is the runtime version; the Temporary Profile is the design-time version. Typically, as you develop a VML profile, you will have a Current Profile that you have trained, accepted, and perhaps deployed to one or more policies, as well as a Temporary Profile that you actively edit and tune.

The Enforce Server administration console displays each version of the VML profile in separate tabs:

#### Current Profile

This version is the active instance of the VML profile. This version has been successfully trained and accepted; it is available for deployment to one or more policies.

Temporary Workspace

This version is an editable version of the VML profile. This version has not been trained, or accepted, or both; it cannot be deployed to a policy.

Initially, when you create a new VML profile, the system displays only the Current Profile tab with an empty training set. After you train and accept the VML profile for the first time, the Trained Set table in the Current Profile tab becomes populated with details about the training set. The information that is displayed in this table and tab is read-only.

#### To edit a VML profile

Click Manage Profile to the far right of the Current Profile tab.

The system displays the editable version of the profile in the **Temporary** Workspace tab. You can now proceed with training and managing the profile.

See "Training VML profiles" on page 518.

The **Temporary Workspace** tab remains present in the user interface until you train and accept a new version of the VML profile. In other words, there is no way to close the Temporary Workspace tab without training and accepting, even if you made no changes to the profile.

Once you accept a new version of the VML profile, the system overwrites the previous Current Profile with the newly accepted version. You cannot revert to a previously accepted Current Profile. However, you can revert to previous versions of the training set for a Temporary Profile.

See "Managing training set documents" on page 521.

## Uploading example documents for training

The training set comprises the example positive and negative documents you want to train the system against. You upload the positive and negative documents separately.

Note: While you can upload individual documents, it is recommended that you upload a document archive (such as ZIP, RAR, or TAR) that contains the recommended (250) or minimum (50) number of example documents. The maximum upload size is 30 MB. You can partition the documents across archives if you have more than 30 MB of data to upload. See "About the content you train" on page 510.

#### To upload the training set

Click **Manage Profile** from the **Current Profile** tab (if you have not already done so).

This action enables the VML profile for editing in the **Temporary Workspace** tab.

See "Working with the Current Profile and Temporary Workspace tabs" on page 515.

2 Click **Upload Contents** (if you have not already done so).

This action opens the **Upload Contents** dialog.

- 3 Select which category of content you are uploading:
  - Choose Positive: match contents similar to these to upload a positive document archive.
  - Choose Negative: ignore contents similar to these to upload a negative document archive.
- Click **Browse** to select the document archive to upload. 4
- 5 Navigate the file system to where you have stored the example documents.
- 6 Choose the file to upload and click **Open**.
- Verify that you have chosen the correct category of content you are uploading: 7 Positive or Negative.
  - If you mismatch the upload (select Negative but upload a Positive document archive), the resulting profile will be inaccurate.
- 8 Click **Submit** to upload the document archive to the Enforce Server.

The system displays a message indicating if the file successfully uploaded. If the upload was successful, the document archive appears in the **New Documents** table. This table displays the document type, name, size, date uploaded, and the user who uploaded it. If the upload was not successful, check the error message and retry the upload. Click the X icon in the Remove column to delete an uploaded document or document archive from the training set.

9 Click **Upload Contents** to repeat the process for the other training set.

The profile is not complete and cannot be trained until you have uploaded the minimum number of positive and negative example documents.

See Table 21-1 on page 511.

10 Once you have successfully uploaded both training sets you are ready to train the VML profile.

See "Training VML profiles" on page 518.

## Training VML profiles

During the profile training process, the system scans the training content, extracts key features, and generates a statistical model. When the training process completes successfully, the system prompts you to accept or reject the training profile. If you accept the training results, that version of the VML profile becomes the Current Profile, meaning that it is active and available for use in one or more policies.

See "Configuring VML profiles and policy conditions" on page 513.

Training the VML profile **Table 21-5** 

Step	Action	Description
Step 1	Enable training mode.	Select the VML profile you want to train from the Manage > Data Profiles > Vector Machine Learning screen. Or, create a new VML profile.
		See "Creating new VML profiles" on page 515.
		Click <b>Manage Profile</b> to the far right of the <b>Current Profile</b> tab. The system displays the profile for training in the <b>Temporary Workspace</b> tab.
		See "Working with the Current Profile and Temporary Workspace tabs" on page 515.
Step 2	Upload the training	Familiarize yourself with the training set requirements and recommendations.
	content.	See "About the content you train" on page 510.
		Upload the positive and negative training sets in separate document archives to the Enforce Server.
		See "Uploading example documents for training" on page 516.

**Table 21-5** Training the VML profile (continued)

Step	Action	Description
Step 3	Adjust the memory allocation (only if necessary).	The default value is "High" which generally results in the best training set accuracy rates. Typically you do not need to change this setting. For some situations you may want to choose a "Medium" or "Low" memory setting (for example, deploying the profile to the endpoint).
		See "Adjusting memory allocation" on page 520.
		<b>Note:</b> If you change the memory setting, you must do so before you train the profile to ensure accurate training results. If you have already trained the profile, you must retrain it again after you adjust the memory allocation.
Step 4	Start the training	Click Start Training to begin the profile training process.
	process.	During the training process, the system:
		<ul><li>Extracts the key features from the content;</li><li>Creates the model;</li></ul>
		<ul> <li>Calculates the predicted accuracy based on the averaged false positive and false negative rates for the entire training set;</li> <li>Generates the VML profile.</li> </ul>
Step 5	Verify training completion.	When the training process completes, the system indicates if the training profile was successfully created.
		If the training process failed, the system displays an error. Check the debug log files and restart the training process.
		See "Debug log files" on page 247.
		On successful completion of the training process, the system displays the following information for the <b>New Profile</b> :
		<ul> <li>Trained Example Documents</li> <li>The number of example documents in each training set that the system trained against and profiled.</li> <li>Accuracy Rate From Training</li> </ul>
		The quality of the training set expressed as base false positive and base false negative percentage rates.  See "About the base accuracy from training percentage rates" on page 511.
		■ Memory
		■ The minimum amount of memory required to load the profile at runtime for detection.
		Note: If you previously accepted the profile, the system also displays the Current Profile statistics for side-by-side comparison.

**Table 21-5** Training the VML profile (continued)

Step	Action	Description
Step 6	Accept or reject the training profile.	If the training process is successful, the system prompts you to accept or reject the training profile. Your decision is based on the <b>Accuracy Rate from Training</b> percentages.
		See "About the base accuracy from training percentage rates" on page 511.
		To accept or reject the training profile:
		<ul> <li>Click Accept to save the training results as the active Current Profile.         Once you accept the training profile, it appears in the Current Profile tab and the Temporary Workspace tab is removed.</li> <li>Click Reject to discard the training results.         The profile remains in the Temporary Workspace tab for editing. You can adjust one or both of the training sets by adding or removing documents and retraining the profile.         See "Managing training set documents" on page 521.</li> </ul>
		<b>Note:</b> A trained VML profile is not active until you accept it. While the system lets you create a policy based on a VML profile that has not been trained or accepted, the VML profile is not deployed to that policy until the profile is accepted. See "About using unaccepted VML profiles in policies" on page 513.
Step 7	Test and tune the profile.	Once you have successfully trained and accepted the VML profile, you can now use it to define policy rules and tune the VML profile.
		See "Configuring the Detect using Vector Machine Learning Profile condition" on page 525.
		See "About the Similarity Threshold and Similarity Score" on page 512.
		Note: For more information, refer to the Symantec Data Loss Prevention Vecctor Machine Learning Best Practices Guide, available at the DLP Knowledgebase (https://kb-vontu.altiris.com/), article number 54340.

## Adjusting memory allocation

The Memory Allocation setting determines the amount of memory required to load VML the profile at runtime for policy detection. The more memory allocated to training the larger the VML profile will be because more features will be modeled. By default this value is set to "High." In general you should not adjust this value. However, if you intend to deploy the VML profile to the endpoint, where resources may be limited, you may want to use a lower memory setting to reduce the size of the profile.

#### To adjust memory allocation

Click **Adjust** beside the **Memory Allocation** setting.

This setting is available in the **Temorary Workspace** tab. If it is not available, click Manage Profile from the Current Profile tab.

See "Working with the Current Profile and Temporary Workspace tabs" on page 515.

2 Select the desired memory allocation level.

The following options are available:

#### High

Requires a higher amount of runtime memory; generally yields higher detection accuracy (default setting).

- Medium
- Low

Requires less runtime memory; may result in lower detection accuracy.

Click **Save** to save the setting. 3

The **Memory Setting** display should reflect the adjustment you made.

4 Click **Start Training** to start the training process.

You must adjust the memory allocation before you train the VML profile. If you have already trained the profile, retrain after adjusting this setting.

See "Training VML profiles" on page 518.

5 Verify the amount of memory required to run the VML profile.

After you train the VML profile, the system displays the Memory Required (KB) value, which represents the minimum amount of memory required to load the profile at runtime.

See "Managing VML profiles" on page 522.

## Managing training set documents

As you train and tune a VML profile, you may need to adjust one or both of the training sets. For example, if you reject a training profile, you will need to add or remove example documents to improve the training accuracy rates.

See "About the base accuracy from training percentage rates" on page 511.

#### To add documents to a training set

Click Manage Profile for the profile you want to edit.

The editable profile appears in the **Temporary Workspace** tab.

2 Click Upload Contents.

See "Uploading example documents for training" on page 516.

#### To remove documents from a training set

Click **Manage Profile** for the profile you want to edit.

The editable profile appears in the **Temporary Workspace** tab.

2 Click the red X in the Mark Removed column for the trained document you want to remove.

The removed document appears in the **Removed Documents** table. Repeat this process as necessary to remove all unwanted documents from the training set.

Click **Start Training** to retrain the profile.

You must retrain and accept the updated profile to complete the document removal process. If you do not accept the new profile the document you attempted to remove remains part of the profile.

See "Training VML profiles" on page 518.

#### To revert removed documents

- 1 Click the revert icon in the Revert column for a document you have removed. The document is added back to the training set.
- 2 Click **Start Training** to retrain the profile.

You must retrain the profile and reaccept it even though you reverted to the original configuration.

## Managing VML profiles

The Manage > Data Profiles > Vector Machine Learning screen is the home page for managing existing VML profiles and the starting point for creating new VML profiles.

See "Configuring VML profiles and policy conditions" on page 513.

Note: You must have Enforce Server administrator privileges to manage and create VML profiles.

Table 1 Creating and managing VML profiles

Action	Description
Create new profiles.	Click <b>New Profile</b> to create a new VML profile.
	See "Creating new VML profiles" on page 515.
View and sort profiles.	The system lists all existing VML profiles and their state at the <b>Vector Machine Learning</b> screen.
	Click the column header to sort the VML profiles by name or status.
Manage and train	Select a VML profile from the list to display and manage it.
profiles.	The Current Profile tab displays the active profile.
	See "Working with the Current Profile and Temporary Workspace tabs" on page 515.
	Click Manage Profile to edit the profile.
	The editable profile appears in the <b>Temporary Workspace</b> tab. From this tab you can:
	<ul> <li>Upload training set documents.</li> <li>See "Uploading example documents for training" on page 516.</li> <li>Train the profile.</li> <li>See "Training VML profiles" on page 518.</li> <li>Add and remove documents from the training sets.</li> </ul>
	See "Managing training set documents" on page 521.
Monitor profiles.	The system lists and describes the status of all VML profiles.
	<ul> <li>Memory Required (KB)         The minimum amount of memory required to load the profile in memory for detection.         See "Adjusting memory allocation" on page 520.     </li> <li>Status         The present status of the profile.         See Table 21-7 on page 524.     </li> </ul>
	■ Deployment Status  The historical status of the profile.  See Table 21-8 on page 524.
Remove profiles.	Click the X icon at the far right to delete an existing profile.  If you delete an existing profile, the system removes the profile metadata and the Training Set from the Enforce Server.

The **Status** field displays the current state of each VML profile.

Status value	Description
Accepted on <date></date>	The date the training profile was accepted.
Managing	The current profile is enabled for editing.
Empty	The profile is created, but no content is uploaded.
Awaiting Acceptance	The profile is ready to be accepted.
Canceling Training	The system is in the process of canceling the training.
Training Canceled	The training process is canceled.
Failed	The training process failed.
Training <time></time>	The training is in progress (for the time indicated).

**Table 21-7** Status values for VML profiles

The **Deployment Status** field indicates if the VML profile has ever been accepted or not.

**Table 21-8** Deployment Status values for VML profiles

Status value	Description
Never Accepted	The VML profile has never been accepted.
	See "About using unaccepted VML profiles in policies" on page 513.
Accepted on <date></date>	The VML profile was accepted on the date indicated.

## Changing names and descriptions for VML profiles

If necessary you can change the name of a VML profile or edit its description. For example, when you are ready to deploy a VML profile to one or more policies, you may want to give the profile a more self-describing name so policy authors can easily recognize it.

Note: You do not have to retrain a profile if you change the name or description.

#### To change the VML profile name or description

1 Select the VML profile from the Manage > Data Profiles > Vector Machine Learning screen.

See "Managing VML profiles" on page 522.

- 2 Click the **Edit** link beside the name of the VML profile.
- Edit the name and description of the profile in the Change Name and **Description** dialog that appears.
- 4 Click **OK** to save the changes to the VML profile name or description.
- 5 Verify the changes at the home screen for the VML profile.

## Configuring the Detect using Vector Machine Learning Profile condition

Once you have trained and accepted the VML profile, you configure a VML policy using the **Detect using Vector Machine Learning Profile** condition. This condition references the VML profile to detect content that is similar to the example content you have trained against.

See "Configuring VML profiles and policy conditions" on page 513.

Configuring a VML policy rule **Table 21-9** 

Step	Action	Description
Step 1	Create and train the VML profile.	See "Creating new VML profiles" on page 515.  See "Training VML profiles" on page 518.  See "About using unaccepted VML profiles in policies" on page 513.
Step 2	Configure a new or an existing policy.	See "Configuring policies" on page 326.
Step 3	Add the VML rule to the policy.	From the Configure Policy screen:  Select Add Rule.  Select the Detect using Vector Machine Learning profile rule from the list of content rules.  Select the VML profile you want to use from the drop-down menu.  Click Next.
Step 4	Configure the VML detection rule.	Name the rule and configure the rule severity.  See "Configuring policy rules" on page 330.

Step	Action	Description
Step 5	Select components to match on.	Select one or both message components to Match On:  Body, which is the content of the message
		■ Attachments, which are any files transported by the message
		<b>Note:</b> On the endpoint, the Symantec DLP Agent matches on the entire message, not individual message components.
		See "Selecting components to match on" on page 336.
Step 6	Configure additional conditions (optional).	Optionally, you can create a compound detection rule by adding more conditions to the rule.
		To add additional conditions, select the desired condition from the drop-down menu and click <b>Add</b> .
		Note: All conditions must match for the rule to trigger an incident.
		See "Configuring compound match conditions" on page 342.
Step 7	Save the policy configuration.	Click <b>OK</b> then click <b>Save</b> to save the policy.

**Table 21-9** Configuring a VML policy rule (continued)

## Configuring VML policy exceptions

In some situations, you may want to implement a VML policy exception to ignore certain content.

See "Configuring VML profiles and policy conditions" on page 513.

Table 21-10 Configuring a VML policy exception

Step	Action	Description
Step 1	Create and train the VML profile.	See "Creating new VML profiles" on page 515. See "Training VML profiles" on page 518.
Step 2	Configure a new or an existing policy.	See "Configuring policies" on page 326.
Step 3	Add a VML exception to the policy.	From the Configure Policy screen:  Select Add Exception.  Select the Detect using Vector Machine Learning profile exception from the list of content exceptions.  Select the VML profile you want to use from the drop-down menu.  Click Next.

Step	Action	Description
Step 4	Configure the policy exception.	Name the exception.  Select the components you want to apply the exception to:  Entire Message Select this option to compare the exception against the entire message. If an exception is found anywhere in the message, the exception is triggered and no matching occurs.  Matched Components Only Select this option to match the exception against the same component as the rule. For example, if the rule matches on the Body and the exception occurs in an attachment, the exception is not triggered.
Step 5 Step 6	Configure the condition.  Save the policy configuration.	Generally you can accept the default condition settings for policy exceptions.  See "Configuring policy exceptions" on page 340.  Click <b>OK</b> then click <b>Save</b> to save the policy.

Configuring a VML policy exception (continued) Table 21-10

## Adjusting the Similarity Threshold

You adjust the Similarity Threshold setting to tune the VML profile. The Similarity Threshold determines how similar detected content must be to a VML profile to produce an incident.

See "About the Similarity Threshold and Similarity Score" on page 512.

Note: You do not have to retrain the VML profile after you adjust the Similarity Threshold, unless you modify a training set based on testing results.

#### To adjust the Current Value of the Similarity Threshold

Click Edit beside the Similarity Threshold label for the VML profile you want to tune.

This action opens the **Similarity Threshold** dialog.

2 Drag the meter to the desired **Curent Value** setting.

You set the Similarity Threshold to a decimal value between 0 and 10. The default value is 10, which produces fewer incidents; a setting of 0 produces more incidents.

- 3 Click **Save** to save the Similarity Threshold setting.
- 4 Test the VML profile using a VML policy.

Compare the Similarity Scores across matches. A detected message must have a Similarity Score higher than the Similarity Threshold to produce an incident. Make further adjustments to the Similarity Threshold setting as necessary to optimize and fine-tune the VML profile.

See "Configuring the Detect using Vector Machine Learning Profile condition" on page 525.

## Testing and tuning VML profiles

You tune a VML profile by testing it with the Similarity Threshold set to 0. Once you determine the possible range of Similarity Scores for false positives, you adjust the Similarity Threshold to be just above the highest Similarity Score reported by false positives. This is referred to as negative testing.

A good training set has a well-defined range where the Similarity Threshold is set to achieve the best accuracy rates. A poor training set yields poor accuracy results regardless of the Similarity Threshold. A Similarity Threshold that is set too high or too low can result in a large number of false positives or false negatives.

To determine the proper Similarity Threshold setting, the recommendation is to perform negative testing as described in the following steps.

Table 21-11 Steps for tuning VML profiles

Step	Action	Description	
Step 1	Train the VML profile.	Follow the recommendations set forth in this guide for defining the category and uploading the training set documents. Adjust the memory allocation before you train the profile. Refer to the <i>Symantec Data Loss Prevention Administration Guide</i> for help performing the tasks involved.	
Step 2	Set the Similarity Threshold to 0.	The default Similarity Threshold is $10$ . At this value the system does not generate any incidents. A setting of $0$ produces the most amount of incidents, many of which are likely to be false positives. The purpose of setting the value to $0$ is to see the entire range of potential matches and to tune the profile to be just above the highest false positive score.	
Step 3	Create a VML policy.	Create a policy that references the VML profile you want to tune. The profile must be accepted to be deployable to a policy.	

Step	Action	Description
Step 4	Test the policy.	Test the VML policy using a corpus of test data. For example, you can use the <code>DLP_Wikipedia_sample.zip</code> file to test your VML policies against. Create some mechanism to detect incidents, such as a Discover scan target of a local file folder where you place the test data, or a DLP Agent scan of a copy/paste operation.
Step 5	Review any incidents.	Review any matches at the Incident Snapshot screen. Verify a relatively low Similarity Score for each match. A relatively low Similarity Score indicates a false positive. If one or more test documents produce a match with a relatively high Similarity Score, you have a training set quality issue. In this case you need to review the content and if appropriate add the document(s) to the positive training set. You then need to retrain and retune the profile.  See "Log files for troubleshooting VML training and policy detection" on page 531.
Step 6	Adjust the Similarity Threshold.	By reviewing the incidents you should now be able to determine the highest Similarity Score among the detected false positives that you have tested the profile against. At this point you can adjust the Similarity Threshold for the profile to be just above the highest Similarity Score for the false positives.  For example, if the highest detected false positive has a Similarity Score of 4.5, set the Similarity Threshold to 4.6. This will filter the known false positives from being reported as incidents.

Table 21-11 Steps for tuning VML profiles (continued)

## Properties for configuring training

VML includes several property files for configuring VML training and logging. The following table lists and describes relevant VML configuration properties.

Property files for VML Table 21-12

Property file at \Protect\config\	Description
MLDTraining.properties	Main property file for configuring VML training settings.  See Table 21-13 on page 530.
Manager.properties	Property file for the Enforce Server; contains 1 VML setting.  See Table 21-14 on page 531.
MLDTrainingLogging.properties	Properties file for configuring VML logging.  See "Log files for troubleshooting VML training and policy detection" on page 531.

The following table lists and describes the VML training parameters available for configuration in properties file MLDTraining.properties.

Relevant configuration parameters for VML training Table 21-13

Parameter	Description
minimum_documents_per_category	Specifies the minimum number of documents required for each training set (positive and negative). The default setting is 50. Reducing this number below 50 is not recommended or supported.
	See "Recommendations for training set definition" on page 535.
mld_num_folds	Specifies the number of folds to use for the k-fold evaluation process. The default is 10.
	Reducing this value will speed up the time the system takes to train against the content because less folds will be evaluated, but potentially at the sacrifice of visibility into profile quality. There is no need to change this value, unless you have a large number of example documents (and thus the training sets are very large), and you know for certain that you have a well-categorized overall training set.
	See "Recommendations for accepting or rejecting a profile" on page 538.
minimum_features_to_keep	Specifies the minimum number of features to keep for the profile. The default setting is 1000.
	Lowering this value can help reduce the size of the profile. However, adjusting this setting is not recommended. Instead, use the memory allocation setting to tune the size of the profile.
	See "Guidelines for profile sizing" on page 537.
significance_threshold	Specifies the minimum number of times a word must occur before it is considered a feature. The default is 2.
	Increasing this value (to 3 or 4, for example) may help reduce the size of the profile because fewer words will qualify as features. In general you should not adjust this setting unless setting the memory allocation to "Low" does not produce a small enough profile for your deployment requirements.
	See "Guidelines for profile sizing" on page 537.

Parameter	Description
stopword_file	Specifies the default stopword file \config\machinelearningconfig\stopwords.txt.
	Stopwords are common words, such as articles and prepositions. During training the system ignores (does not consider for feature extraction) any word contained in the stopwords file.
	If you add words to be ignored, you must use all lower case because VML feature extraction normalizes the content to lower case for evaluation.
logging_config_file	Specifies the configuration file for standard VML logging.  See "Log files for troubleshooting VML training and policy detection" on page 531.
native_logging_config_file	Specifies the configuration file for native VML logging.  See "Log files for troubleshooting VML training and policy detection" on page 531.

Table 21-13 Relevant configuration parameters for VML training (continued)

The following parameter is available for configuration in properties file MLDTraining.properties.

Table 21-14 Configuration parameter for VML profiles

Parameter	Description
DEFAULT_SIMILARITY_THRESHOLD	Establishes the default value for the Similarity Threshold, which is 10. Changing this value affects the default value only. You can adjust the value using the Enforce Server administration console.
	See "Testing and tuning VML profiles" on page 528.

## Log files for troubleshooting VML training and policy detection

The system provides debug log files for troubleshooting the VML training process and policy detection. The following table lists and describes the debug log files.

See "Troubleshooting policies" on page 353.

Table 21-15 Debug log files for VML

Log file	Description	
machinelearning_training.log	Records the accuracy from training percentage rates for each fold of the evaluation process for each VML profile training run.	
	This log file is useful for examining the quality of each training set at a granular, per-fold level.	
	See "Recommendations for accepting or rejecting a profile" on page 538.	
machinelearning native filereader.log	Records the "distance," which is expressed as a positive or negative number, and the "confidence," which is a similarity percentage, for each message evaluated by a VML policy.	
	This log file is useful for examining all messages or documents evaluated by VML policies, including positive matches with similarity percentages beneath the Similarity Threshold, or messages the system has categorized as negative (expressed as a negative "distance" number).	
	See "Testing and tuning VML profiles" on page 528.	
machinelearning_training_native_manager.log	Records the total number of features modeled and the number of features kept to generate the profile for each training run.	
	The total number of features modeled versus the number of features kept for the profile depends on the memory allocation setting:	
	<ul> <li>If "high" the system keeps 80% of the features.</li> <li>If "medium" the system keeps 50% of the features.</li> <li>If "low" the system keeps 30% of the features.</li> </ul>	
	See "Guidelines for profile sizing" on page 537.	

# Best practices for using VML

This section provides best practices for implementing VML policies, including best practices for testing and tuning your VML policies.

In addition, you can download example VML training set documents from the DLP Knowledgebase (https://kb-vontu.altiris.com), article number 54340. These documents are provided under the Creative Commons license (http://creativecommons.org/licenses/by-sa/3.0/).

The following table provides a summary of the VML best practices discussed in this section, with links to individual topics for more in-depth recommendations.

Table 21-16 Summary of VML best practices

Functional area	Best practice	
Recommended uses for VML	Use VML to protect unstructured, text-based content. Do not use VML to protect graphics, binary data, or personally identifiable information (PII).	
	See "When to use VML" on page 533.	
Category of content	Define the VML profile based on a single category of content that you want to protect and that is derived from a specific business use case. Narrowly defined categories are better than broadly defined ones.	
	See "Recommendations for training set definition" on page 535.	
Positive training set	Archive and upload the recommended (250) number of example documents for the positive training set, or at least the minimum (50).	
	See "Guidelines for training set sizing" on page 536.	
Negative training set	Archive and upload the example documents for the negative training set. Ideally the negative training set contains a similar number of well-categorized documents as the positive training set. In addition, add some documents containing generic or neutral content to your negative training set.	
	See "Guidelines for training set sizing" on page 536.	
Profile sizing	Consider adjusting the memory allocation to low. Internal testing has shown that setting the memory allocation to low may improve accuracy in certain cases.	
	See "Guidelines for profile sizing" on page 537.	
Training set quality	Reject the training result and adjust the example documents if either of the base accuracy rates from training are more than 5%.	
	See "Recommendations for accepting or rejecting a profile" on page 538.	
Profile tuning	Tune the VML profile by performing negative testing using a corpus of testable data.	
	See "Testing and tuning VML profiles" on page 528.	
Profile deployment	Remove accepted profiles not in use by policies to reduce detection server load. Tune the Similarity Threshold before deploying a profile into production across all endpoints to avoid network overhead.	
	See "Recommendations for deploying profiles" on page 540.	

## When to use VML

VML is designed to protect unstructured content that is primarily text-based. VML is well-suited for protecting sensitive content that is highly distributed such that gathering all of it for fingerprinting is not possible or practical. VML is also well-suited for protecting sensitive content that you cannot adequately describe and achieve high matching accuracy.

The following table summarizes the recommended uses cases for VML.

Recommended uses for VML Table 21-17

Use VML when	Explanation	
It is not possible or practical to fingerprint all the data you want to protect.	Often collecting all of the content you want to protect for fingerprinting is an impossible task. This situation arises for many forms of unstructured data: marketing materials, financial documents, patient records, product formulas, source code, and so forth.  VML works well for this situation because you do not have to collect all of the content you want to protect, only a smaller set of example documents.	
You cannot adequately describe the data you want to protect.	Often describing the data you want to protect is difficult without sacrificing some accuracy. This situation may arise when you have long keyword lists that are hard to generate, tune, and maintain.	
	VML works well in these situations because it automatically models the features (keywords) you want to protect, and lets you easily manage and update the source content.	
A policy reports frequent false positives.	Sometimes a certain category of information is a constant source of false positives.  For example, a weekly sales report may consistently produce false positives for a Data Identifier policy looking for social security numbers.	
	VML may work well here because you can train against the content that causes the false positives and create a policy exception to ignore those features.	
	<b>Note:</b> The false positive contents must belong to a well-defined category for VML to be an effective solution for this use case. See "Recommendations for training set definition" on page 535.	

## When not to use VML

VML is not designed to protect structured data, such as Personally Identifiable Information (PII), or binary content, such as documents that contain mostly graphics or image files.

The following table summarizes the non-recommended uses of VML.

Non-recommended uses for VML Table 21-18

Do not use VML to	Explanation
Protect personally identifiable information (PII).	Exact Data Matching (EDM) and Data Identifiers are the best option for protecting the common types of PII.

Do not use VML to

Explanation

Protect binary files and images.

Indexed Document Matching (IDM) is the best option to protect content that is largely binary, such as image files or CAD files.

**Table 21-18** Non-recommended uses for VML (continued)

## Recommendations for training set definition

A VML category is the specific business use case from which you derive your example documents for training the VML profile. The more specific the category the better the detection results. For example, the category "Financial Documents" is not recommended because it is too broad. A better category classification is "Sales Forecasts" or "Quarterly Earnings" because each is particular to a specific business use case.

A VML category contains two sets of training content: positive and negative. The positive training set contains content you want to protect; the negative training set contains content you want to ignore. You should derive both the positive and negative training sets from the same category of content such that all documents are thematically related.

While it is possible to use entirely generic content for the negative training set, this is not recommended. A completely generic negative training set may produce good design-time training accuracy rates, but it is likely that at runtime you will not be able to detect the content you want to protect with sufficient accuracy.

**Note:** While a completely generic negative training set is not recommended, seeding the negative training set with some neutral-content documents does have value. See "Guidelines for training set sizing" on page 536.

The following table provides some example categories and possible positive and negative training sets comprising those categories.

**Table 21-19** Some example categories and training sets

Category	Positive training set	Negative training set
Product Source Code	Proprietary product source code	Source code from open source projects
Product Formulas	Proprietary product formulas	Non-proprietary product information
Quarterly Earnings	Pre-release earnings; sales estimates; accounting documents	Details of published annual accounts

Category	Positive training set	Negative training set
Marketing Plans	Marketing plans	Published marketing collateral, advertising copy
Medical Records	Patient medical records	Healthcare documents
Customer Sales	Customer purchasing patterns	Publicly available consumer data
Mergers and Acquisitions	Confidential legal documents; M&A documents	Publicly available materials; press releases
Manufacturing Methods	Proprietary manufacturing methods and research	Industry standards

Table 21-19 Some example categories and training sets (continued)

## Guidelines for training set sizing

VML is only as accurate as the example content you train. Unlike other detection technologies, to use VML you do not have to locate all the data you want to protect, nor do you have to describe it. But, you must select example documents that accurately represent the type of content you want to protect, as well as content you want to ignore that is thematically related to the positive content.

The more example documents you collect for training the more accurate the VML profile will be. A well-defined category of content contains 500 example documents: 250 positive and 250 negative. The minimum number of documents per training set is 50.

Ideally you will collect for training a similar number of negative documents as positive. However, this is not always possible. Regardless of how many negative documents you collect, you should seed the negative training set with generic or neutral-content documents. The archive file DLP Wikipedia sample.zip that is attached to this guide at the Knowledgebase is provided for this purpose. For example, if your positive training set contains the recommended number of example documents (250), and the negative training set contains 150 documents, you could add 100 to 200 generic documents to your negative training set from the DLP Wikipedia sample.zip archive file. Internal testing has shown that adding generic content to complement an otherwise well-defined negative training set can improve accuracy for VML.

If you cannot collect enough positive documents to meet the minimum requirement, you can upload the under-sized training set multiple times. For example, consider a case where you have the category of content "Sales Forecasts." For this category you have collected 25 positive spreadsheets and 50 negative documents. In this case, you could upload the positive training set twice to reach the minimum

document threshold and equal the number of negative documents. Note that you should use this technique for development and testing purposes only. Production profiles should be trained against at least the minimum number of documents for both training sets.

The table below lists the optimal, recommended, and minimum number of documents to include in each training set.

Note: These training set guidelines assume an average document size of 3 KB. If you have larger-sized documents, fewer in number may be sufficient.

Training set	Minimum	Recommended
Positive example documents	50	250
Negative example documents	50	250
Total number of documents for the category	100	500

Table 21-20 Training set size guidelines

## Recommendations for uploading documents for training

While you can upload individual documents to the Enforce Server for training, it is recommended that you upload a document archive (ZIP, RAR, TAR) that contains the example documents for each training set. The maximum upload size is 30 MB. There is no training set size limit.

To gather the documents for training, it is recommended that you create a staging area. For example, consider a category called "Sales Reports." In this case you would create a folder called \VML\training stage\sales reports that represents the category. Within this folder you would create two subfolders, one for the positive training set and the other for the negative training set (for example:

\VML\training stage\sales reports\positive). When you are ready to train the profile, you compress the positive subfolder and the negative subfolder into separate document archives. You can partition the training set across archives if you have more than 30 MB of data to upload for a training set. Do not embed an archive within an archive.

## Guidelines for profile sizing

Before you train a VML profile, you can adjust the amount of memory allocated to the profile. The amount of memory you allocate determines how many features the system models, which in turn affects the size of the profile. The higher the memory allocation setting, the more in-depth the feature extraction and the plotting of the model, and the larger the profile. In general, for server-based policy detection, the recommended memory allocation setting is high, which is the default setting.

On the endpoint, the VML profile is deployed to the host computer and loaded into memory by the DLP Agent. (Unlike EDM and IDM, VML does not rely on two-tier detection for endpoint policies.) Because memory on the endpoint is limited, the recommendation is to allocate low or medium memory for endpoint policies. Internal testing has shown that reducing the memory allocation does not reduce the accuracy of the profile and may improve accuracy in certain situations.

Memory allocation	Description	
High	Default setting generally appropriate for server-based detection.	
Medium	Use this setting to reduce the size of the profile.	
Low	Use this setting for endpoint detection.	

 Table 21-21
 Memory allocation recommendations

## Recommendations for accepting or rejecting a profile

When you train a VML profile against the category content, the system selects features, creates the model, and calculates the base accuracy rates for false positives and negatives. Base accuracy rates are calculated using a standard and generally accepted process called k-folds evaluation. The base accuracy rates provide you with an early indicator of the quality of your category training sets.

To illustrate how the k-folds evaluation process works, assume that you have a category with 500 total example documents: 250 positive and 250 negative. During the training run, the system divides the training set into 10 folds, each of which are distinct subsets of the overall training set and contain both positive and negative example documents. The system uses nine folds to generate a VML profile, and one fold to test the profile. Any of the folds can become the test fold for the first round of evaluation. For the next round, the next fold in the queue becomes the test fold. This process repeats for all 10 folds. The system performs a final training run called the cross-fold, averages the results of all folds, and generates the final model.

On successful completion of the training process, the system displays the averaged accuracy rates and prompts you to accept or reject the training profile. The false positive accuracy rate is the percentage of negative test documents misclassified as positive. The false negative rate is the percentage of positive test documents that are misclassified as negative. As a general guideline, you should reject the training profile if either rate is more than 5%.

Note: You can use the log file machinelearning training.log to evaluate per-fold training accuracy rates.

See "Log files for troubleshooting VML training and policy detection" on page 531.

## Guidelines for accepting or rejecting training results

You decide to accept or reject a training profile based on the false positive and false negative percentages that the system displays to you at the end of the training process.

See "About the Similarity Threshold and Similarity Score" on page 512.

To better understand how the system calculates the Machine Learning Profile training set accuracy rates, consider the following example.

You have a training set that includes 1000 documents, 500 positive and 500 negative. When you train the profile, the system takes 90% of the documents, extracts the features, and creates a model. It takes the remaining 10% of the documents and evaluates their features against the model for similarity, producing false positive and false negative accuracy rates. This process is known as the "fold." For each training set, the system evaluates ten folds, each time comparing a different 10% of the documents against the 90%. At the end of the cycle, the system performs a cross-fold evaluation of all ten folds and produces an average accuracy percentage rate for both the positive and negetaive categories.

Continuing the example, assume the result of the training process yields a base false positive rate of approximately 1.2% and a base false negative rate of approximately 1%. This means that, on average, 1.2% of the negative documents in the training set are miscategorized as positive, and 1% of the documents in the training set are miscategorized as negative. While the goal is 0% for both rates, in general a percentage rate below 5% for each category is acceptable.

However, since, the percentages produced at the end of the training process are averages across the 10 folds, rather than relying on the general 5% rule of thumb, the better practice is to review the percentage rate results for each fold. To do this, examine the log file \Vontu\Protect\logs\debug\mld0.log. As shown below, the individual fold rates give a reading for each of the ten folds on which you can base your decision to accept or reject the profile.

Table 21-22 Training set accuracy evaluation process

Fold evaluation	Per fold category accuracy rates and cross-fold averages	
Fold 0	false positive rate 2.013422727584839	false negative rate 0.0
Fold 1	false positive rate 1.3513513803482056	false negative rate 1.7857142686843872

Fold evaluation	Per fold category accuracy rates and cross-fold averages	
Fold 2	false positive rate 1.3513513803482056	false negative rate 0.8928571343421936
Fold 3	false positive rate 1.3513513803482056	false negative rate 1.7857142686843872
Fold 4	false positive rate 1.3513513803482056	false negative rate 0.8928571343421936
Fold 5	false positive rate 1.3513513803482056	false negative rate 2.6785714626312256
Fold 6	false positive rate 0.0	false negative rate 0.0
Fold 7	false positive rate 0.6756756901741028	false negative rate 0.0
Fold 8	false positive rate 1.3513513803482056	false negative rate 0.8928571343421936
Fold 9	false positive rate 1.3513513803482056	false negative rate 1.8018018007278442
Cross-fold	Avg False Positive Rate 1.214855808019638	Avg False Negative Rate 1.0730373203754424

Table 21-22 Training set accuracy evaluation process (continued)

## Recommendations for deploying profiles

Accepted VML profiles are transferred to every detection server and Symantec DLP Agent even if those profiles are not required by the active policies on that server or endpoint. Detection servers load all VML profiles into memory regardless of whether or not any associated VML policies are deployed to those servers. DLP Agents only load the VML profiles that are required by an active policy. To optimize server performance, it is recommended not to deploy (accept) unnecessary VML profiles and remove any accepted (deployed) VML profiles that are not required by active policies.

In addition, when you change the Similarity Threshold, the system re-syncs the entire profile with the detection servers and DLP Agents. If you have a large VML profile and possible bandwidth limitations (for example, deployment to many endpoints), this may cause network congestion. In this case you should test and tune the profile at a select few endpoints before deploying the profile into production at every endpoint on your network.

# Detecting content using data identifiers

This chapter includes the following topics:

- Introducing data identifiers
- Conifuring data identifier policy conditions
- Modifying system data identifiers
- Creating custom data identifiers
- Best practices for using data identifiers

# Introducing data identifiers

Symantec Data Loss Prevention provides data identifiers to detect specific instances of described content. Data identifiers let you quickly implement precise, short-form data matching with minimal effort.

Data identifiers are algorithms that combine pattern matching with data validators to detect content. Patterns are similar to regular expressions but more efficient because they are tuned to match the data precisely. Validators are accuracy checks that focus the scope of detection and ensure compliance.

For example, the "Credit Card Number" system data identifier detects numbers that match a specific pattern. The matched pattern is validated by a "Luhn check," which is an algorithm. In this case the validation is performed on the first 15 digits of the number that evaluates to equal the 16th digit.

Symantec Data Loss Prevention provides preconfigured data identifiers that you can use to detect commonly used sensitive data, such as credit card, social security, and driver's license numbers. Data identifiers come in three breadths—wide,

medium, and narrow—so you can fine-tune your detection results. Data identifiers offer broad support for detecting international content.

If a system-defined data identifier does not meet your needs, you can modify it. You can also define your own custom data identifiers to detect any content that you can describe.

See "System-defined data identifiers" on page 542.

See "Selecting a data identifier breadth" on page 555.

## System-defined data identifiers

Symantec Data Loss Prevention provides several system-defined data identifiers to help you detect and validate pattern-based sensitive data.

**Table 22-1** System data identifiers

Category	Description
Personal Identity	Detect various types of identification numbers for the regions of North America, Europe, and Asia Pacific.
	See Table 22-2 on page 543.
	See Table 22-3 on page 543.
	See Table 22-4 on page 544.
	See Table 22-4 on page 544.
Financial	Detect financial identification numbers, such as credit card numbers and ABA routing numbers.
	See Table 22-5 on page 545.
Healthcare	Detect U.S. and international drug codes.
	See Table 22-6 on page 545.
Information	Detect IP addresses.
Technology	See "Information technology data identifier" on page 545.
Internation keywords	International keywords for PII data identifiers.
	See "International keywords for PII data identifiers" on page 545.

## Peronal identity data identifiers

Symantec Data Loss Prevention provides various data identifiers for detecting personally identifiable information (PII) for the regions of Asia Pacific, Europe, and North America.

See Table 22-2 on page 543. lists system-defined data identifiers for the Asia Pacific region.

**Table 22-2** Asia Pacific personal identity

Data identifier	Description
Australian Tax File Number	See "Australian Tax File Number data identifier" on page 707.
People's Republic of China ID	See "People's Republic of China ID data identifier" on page 758.
Hong Kong ID	See "Hong Kong ID data identifier" on page 743.
Singapore NRIC	See "Singapore NRIC data identifier" on page 760.
South Korean Resident Registration Number	See "South Korea Resident Registration Number data identifier" on page 761.
Taiwan ID	See "Taiwan ID data identifier" on page 767.

See Table 22-3 on page 543. lists system-defined data identifiers for the European region.

**Table 22-3** European personal identity

Data identifier	Description
Codice Fiscale	See "Codice Fiscale data identifier" on page 712.
Spanish DNI ID	See "Spanish DNI ID data identifier" on page 763.
Burgerservicenummer	See "Burgerservicenummer data identifier" on page 707.
UK Driver's License Number	See "UK Drivers License Number data identifier" on page 768.
UK Tax ID Number	See "UK Tax ID Number data identifier" on page 785.
UK Passport Number	See "UK Passport Number data identifier" on page 781.
UK National Insurance Number	See "UK National Insurance Number data identifier" on page 777.
UK National Health Service (NHS) Number	See "UK National Health Service (NHS) Number data identifier" on page 773.
UK Electoral Roll Number	See "UK Electoral Roll Number data identifier" on page 772.
French INSEE Code	See "French INSEE Code data identifier" on page 742.

**Table 22-3** European personal identity (continued)

Data identifier	Description
Swiss AHV Number	See "Swiss AHV Number data identifier" on page 767.

Table 22-4 lists system-defined data identifiers for the North American region.

North American personal identity **Table 22-4** 

Data identifier	Description
Randomized US Social Security Number (SSN)	See "Randomized US Social Security Number (SSN) data identifier" on page 759.
US Social Security Number (SSN)	See "US Social Security Number (SSN) data identifier" on page 793.
	<b>Note:</b> This data identifer is replaced by the Randomized US SSN data identifier.
Canadian Social Insurance Number	See "Canadian Social Insurance Number data identifier" on page 708.
US Individual Tax ID Number (ITIN)	See "UK Tax ID Number data identifier" on page 785.
Driver's License Number – CA State	See "Drivers License Number – CA State data identifier" on page 730.
Driver's License Number – IL State	See "Drivers License Number - IL State data identifier" on page 735.
Driver's License Number – NJ State	See "Drivers License Number - NJ State data identifier" on page 737.
Driver's License Number – NY State	See "Drivers License Number - NY State data identifier" on page 740.
Driver's License Number – FL, MI, MN States	See "Drivers License Number - FL, MI, MN States data identifier" on page 732.

### Financial data identfiers

Table 22-5 lists system-defined data identifiers for detecting financial identification numbers, such as credit card numbers and ABA routing numbers.

Tuble 22.5 Financial data identifiers		
Data identifier	Description	
Credit Card Number	See "Credit Card Number data identifier" on page 715.	
ABA Routing Number	See "ABA Routing Number data identifier" on page 702.	
CUSIP Number	See "CUSIP Number data identifier" on page 726.	
SWIFT Code	See "SWIFT Code data identifier" on page 764.	
Credit Card Magnetic Stripe Data	See "Credit Card Magnetic Stripe Data data identifier" on page 713.	
IBAN West	See "IBAN West data identifier" on page 748.	
IBAN Central	See "IBAN Central data identifier" on page 743.	
IBAN East	See "IBAN East data identifier" on page 745.	

**Table 22-5** Financial data identifiers

#### Healthcare data identifiers

Table 22-6 lists system-defined data identifiers for detecting U.S. and international drug codes.

Table 22	2-6	Healthcare

Data identifier	Description
National Drug Code	See "National Drug Code (NDC) data identifier" on page 754.
Australian Medicare Number	See "Australian Medicare Number data identifier" on page 706.

## Information technology data identifier

Symantec Data Loss Prevention provides the IP Address data identifier for detecting IP addresses in the IPv4 format. IPv6 formats are not supported.

See "IP Address data identifier" on page 750.

## International keywords for PII data identifiers

Symantec Data Loss Prevention lets you modify system data identifiers and cutomize the input keywords to detect a broad range of international content.

See "Extending and customizing data identifiers" on page 546.

See "Use custom keywords for system data identifiers" on page 606.

## Extending and customizing data identifiers

You can customize data identifiers to suit your requirements. You can extend system-defined data identifiers by modifying them. And, you can create new data identifiers for custom data matching.

The most common use case for modifying a system-defined data identifier is to edit the data input for a validator that accepts data input. For example, if the data identifier implements the "Find keywords" validator, you may want to add or remove values from the list of keywords. Another use case may involve adding or removing validators to or from the data identifier, or changing one or more of the patterns defined by the data identifier.

See "Cloning a system data identifier before modifying it" on page 565.

To create a custom data identifier, you implement one or more detection pattern(s), select one or more data validators, provide the data input if the validator requires it, and choose a data normalizer.

See "Custom data identifier configuration" on page 572.

Policy authors can reuse modified and custom data identifiers in one or more policies.

## About data identifier configuration

You can configure three types of data identifiers:

- Instance defined at the policy level See "Conifuring data identifier policy conditions" on page 549.
- Modified configured at the system-level See "Modifying system data identifiers" on page 564.
- Custom created at the system-level See "Creating custom data identifiers" on page 570.

The type of data identifier you implement depends on your business requirements. For most use cases, configuring a policy instance using a non-modified, system-defined data identifier is sufficient to accurately detect data loss. Should you need to, you can extend a system-defined data identifier by modifying it, or you can implement one or more custom data identifiers to detect unique data.

Data identifier configuration done at the policy instance-level is specific to that policy. Modifications you make to data identifiers at the system-level apply to all data identifiers derived from the modified data identifier.

#### About data identifier breadths

System data identifiers are implemented by breadth. The breadth defines the scope of detection for that data identifier. Each data identifier implements at least one breadth of detection. The widest option available for the data identifier is likely to produce the most false positive matches; the narrowest option produces the least. Generally the validators and often the patterns differ among breadths.

See "Using data identifier breadths" on page 554.

For example, the Driver's License Number – CA State data identifier provides wide and medium breadths, with the medium breadth using a keyword validator.

Note: Not all system data identifiers provide each breadth of detection. Refer to the complete list of data identifiers and breadths to determine what is available.

See "Selecting a data identifier breadth" on page 555.

## About optional validators for data identifiers

Optional validators help you refine the scope of detection for a data identifier. When you configure a data identifier instance, you can select among five optional validators.

See "Using optional validators" on page 558.

The type of characters accepted by each optional validator depends on the data identifier.

See "Acceptable characters for optional validators" on page 560.

Note: Optional validators only apply to the policy instance you are actively configuring; they do not apply system-wide.

## About data identifier patterns

Data identifiers implement patterns to match data. The data identifier pattern syntax is similar to the regular expression language, but more limited. For example, the data identifier pattern syntax does not support some regular expression features, including grouping, lookahead and lookbehind expressions, and many special characters (notably the dot "." character). In addition, the system only allows the use of ASCII characters for data identifier patterns.

See "Using the data identifier pattern language" on page 573.

When you edit a system data identifier, the system exposes the pattern for viewing and editing. The system-defined data identifier patterns have been tuned and optimized for precise content matching.

See "Selecting a data identifier breadth" on page 555.

In addition, you can create a custom data identifier in which case you are required to implement at least one pattern. The best way to understand how to write patterns is to examine the system-defined data identifier patterns.

See "Writing data identifier patterns to match data" on page 574.

## About pattern validators

Pattern validators are validation checks applied to data matched by a data identifier pattern. Validators help refine the scope of detection and reduce false positives. Many validators allow for data input. For example, the Keyword validator lets you enter a list of keywords.

See "Using pattern validators" on page 575.

When you modify a data identifier, you can edit the input values for any validator that accepts data.

See "Editing pattern validator input" on page 566.

When you modify a data identifier, you can add and remove pattern validators. When you create custom data identifiers, you can configure one or more validators. The system also provides you with the ability to author a custom script validator to define your own validation check.

See "Selecting pattern validators" on page 577.

## About data normalizers

A data normalizer reconciles the data detected by the data identifier pattern with the format expected by the normalizer. You cannot modify the normalizer of a system-defined data identifier. When you create a custom data identifier, you select a data normalizer.

See "Acceptable characters for optional validators" on page 560.

See "Selecting a data normalizer" on page 578.

## About cross-component matching

Data identifiers support component matching. This means that you can configure data identifiers to match on one or more message components. However, if the data identifier implements a validator (optional or required), such as Find keywords, the validated data and the matched data must exist in the same component to trigger or except an incident.

See "Detection messages and message components" on page 305.

For example, consider a scenario where you implement the Randomized US Social Security Number (SSN) data identifier. This data identifier detects on various 9-digits patterns and uses a keyword validator to narrow the scope of detection. (The keyword and phrases in the list are "social security number, ssn, ss#"). If the detection engine receives a message with the number pattern 123-45-6789 and the keyword "social security number" and both data items are contained in the message attachment component, the detection engine reports a match. However, if the attachment contains the number but the body contains the keyword validator. the detection engine does not consider this to be a match.

See "Configuring the Content Matches data identifier condition" on page 552.

See "Randomized US Social Security Number (SSN) data identifier" on page 759.

## About unique match counting

Data identifiers support unique match counting. This feature lets you count only those pattern matches that are unique.

Unique match counting is useful when you are only concerned with detecting the presence of unique patterns and not with detecting every matched pattern. For example, you could use unique match counting to trigger an incident if a document contains 10 or more unique social security numbers. In this case, if a document contained 10 instances of the same social security number, the policy would not trigger an incident.

See "Using unique match counting" on page 562.

See "Configuring unique match counting" on page 563.

# Conifuring data identifier policy conditions

Table 22-7 lists and describes the configuration options for data identifier conditions.

See "Introducing data identifiers" on page 541.

See "Configuring the Content Matches data identifier condition" on page 552.

Table 22-7 Pol	licy instance data	identifier configuration
----------------	--------------------	--------------------------

Selectable at the policy level	Not configurable
<ul> <li>Breadth         You can implement any breadth the data identifier supports at the instance level.</li> <li>Optional Validators         You can select one or more optional validators at the instance level.</li> </ul>	<ul> <li>Patterns         You cannot modify the match patterns at the instance level.     </li> <li>Active Validators         You cannot modify, add, or remove required validators at the instance level.     </li> </ul>

## Workflow for configuring data identifier policies

Table 22-8 describes the workflow for implementing system-defined data identifiers.

Workflow for implementing data identifiers **Table 22-8** 

Step	Action	Description
1	Decide the type of data identifier you want to implement.	See "Introducing data identifiers" on page 541.
2	Decide the data identifier breadth.	See "About data identifier breadths" on page 547.
3	Configure the data identifier.	See "Configuring the Content Matches data identifier condition" on page 552.
4	Test and tune the data identifier policy.	See "Best practices for using data identifiers" on page 579.

## Managing and adding data identifiers

The Manage > Policies > data identifiers screen lists all data identifiers, including system- and custom-defined. From this screen you manage and modify existing data identifiers, and add new ones.

See "Introducing data identifiers" on page 541.

Table 22-9	Manage data identifiers
------------	-------------------------

Action	Description
Edit a data identifier.	Select the data identifier from the list to modify it.
	See "Selecting a data identifier breadth" on page 555.
	See "Extending and customizing data identifiers" on page 546.
	See "Editing data identifiers" on page 551.
Define a custom data	Click Add data identifier to create a custom data identifier.
identifier.	See "Custom data identifier configuration" on page 572.
	See "Workflow for creating custom data identifiers" on page 570.
Sort and view data	The list is sorted alphabetical by <b>Name</b> .
identifiers.	You can also sort by the <b>Category</b> .
	A pencil icon to the left means that the data identifier is modified from its original state, or is custom.
Remove a data	Click the X icon on the right side to delete a data identifier.
identifier.	The system does not let you delete system data identifiers. You can only delete custom data identifiers.

## Editing data identifiers

You can modify system-defined data identifiers, including the patterns, validators, and validator input. Modifications are propagated to any policy that declares the data identifier. You cannot rename a system data identifier. Consider manually creating a cloned copy before you modify a system data identifier.

See "Extending and customizing data identifiers" on page 546.

Note: The system does not export data identifiers in a policy template. The system exports a reference to the system data identifier. The target system where the policy template is imported provides the actual data identifier. If you modify a system-defined data identifier, the modifications do not export to the template.

Table 22-10 Workflow for editing data identifiers

Step	Action	Description
Step 1	Clone the system data identifer	Clone the system data identifier before you modify it.
	you want to modify.	See "Cloning a system data identifier before modifying it" on page 565.
		See "Clone system-defined data identifiers before modifying to preserve original state" on page 581.
Step 2	Edit the cloned data identifier.	If you modify a system data identifier, click the plus sign to display the breadth and edit the data identifier.
		See "Selecting a data identifier breadth" on page 555.
Step 3	Edit one or more <b>Patterns</b> .	You can modify any pattern that the Data Identifier provides.
		See "Writing data identifier patterns to match data" on page 574.
Step 4	Edit the data input for any	See "Editing pattern validator input" on page 566.
	validator that accepts input.	See "List of pattern validators that accept input data" on page 566.
Step 5	Optionally, you can add or remove <b>Validators</b> , as necessary.	See "Selecting pattern validators" on page 577.
Step 6	Save the data identifier.	Click <b>Save</b> to save the modifications.
		Once the data identifier is saved, the icon at the <b>Data Identifiers</b> screen indicates that it is modified from its original state, or is custom.
		See "Managing and adding data identifiers" on page 550.
		Note: Click Cancel to not save the Data Identifier.
Step 7	Implement the data identifier in a policy rule or exception.	See "Configuring the Content Matches data identifier condition" on page 552.

## Configuring the Content Matches data identifier condition

You can configure the Content Matches data identifier condition in policy detection rules and exceptions.

See "Introducing data identifiers" on page 541.

Configuring the Content Matches data identifier condition Table 22-11

Step	Action	Description
Step 1	Add a data identifier rule or exception to a policy, or configure an existing	Select the Content Matches data identifier condition at the Add Detection Rule or Add Exception screen.  See "Adding a rule to a policy" on page 328.
	one.	See "Adding an exception to a policy" on page 337.
Step 2	Choose a data identifier.	Choose a data identifier from the list and click <b>Next</b> .
		See "System-defined data identifiers" on page 542.
Step 3	Select a <b>Breadth</b> of	Use the breadth option to narrow the scope of detection.
	detection.	See "About data identifier breadths" on page 547.
		Wide is the default setting and detects the broadest set of matches. Medium and narrow breadths, if available, check additional criteria and detect fewer matches.
		See "Selecting a data identifier breadth" on page 555.
Step 4 Select and configure one or more <b>Optional Validators</b> .		Optional validators restrict the match criteria and reduce false positives.
		See "About optional validators for data identifiers" on page 547.
Step 5	Configure Match	Select how you want to count matches:
	Counting.	■ Check for existence  Do not count multiple matches; report a match count of 1 for one or more matches.
		■ Count all matches
		Count each match; specify the minimum number of matches to report an incident.
		See "Configuring match counting" on page 334.
		Count all unque matches  This is the default acting for version 44.0 and higher
		This is the default setting for version 11.6 and higher.  See "About unique match counting" on page 549.
		See "Configuring unique match counting" on page 563.

Table 22-11 Configuring the Content Matches data identifier condition (continued)

Step	Action	Description
Step 6	Configure the message	Select one or more message components on which to match.
	components to Match On.	On the endpoint, the detection engine matches the entire message, not individual components.
		See "Selecting components to match on" on page 336.
		If the data identifier uses optional or required keyword validators, the keyword must be present in the same component as the matched data identifier content.
		See "About cross-component matching" on page 548.
Step 7	Configure additional conditions to Also Match.	Optionally, you can <b>Add</b> one or more additional conditions from any available in the <b>Also Match</b> condition list.
		All conditions in a compound rule or exception must match to trigger or except an incident.
		See "Configuring compound match conditions" on page 342.

# Using data identifier breadths

Each system data identifier provides one or more breadths of detection. When you configure a system data identifier instance, or when you modify a system data identifier, you select which breadth to implement. Not all breadth options are available for each data identifier.

See "About data identifier breadths" on page 547.

Available rule breadths for system data identifiers **Table 22-12** 

Breadth	Description
Wide	The wide breadth defines a single or multiple patterns to create the greatest number of matches. In general this breadth produces a higher rate of false positives than the medium and narrow breadths.
Medium	The medium breadth may refine the detection pattern(s) and/or add one or more data validators to limit the number of matches.
Narrow	The narrow breadth offers the tightest patterns and strictest validation to provide the most accurate positive matches. In general this option requires the presence of a keyword or other validating restriction to trigger a match.

## Selecting a data identifier breadth

You cannot change the normalizer that a system data identifier implements. This information is useful to know when you implement one or more optional validators.

See "Acceptable characters for optional validators" on page 560.

System data identifier breadths and normalizers Table 22-13

data identifier	Breadth(s)	Normalizer
ABA Routing Number	Wide	Digits Only
See "ABA Routing Number data identifier" on page 702.	Medium	
	Narrow	
Australian Medicare Number	Wide	Digits Only
See "Australian Medicare Number data identifier" on page 706.		
Australian Tax File Number	Wide	Digits Only
See "Australian Tax File Number data identifier" on page 707.		
Burgerservicenummer	Wide	Digits Only
See "Burgerservicenummer data identifier" on page 707.		
Canadian Social Insurance Number	Wide	Digits Only
See "Canadian Social Insurance Number data identifier"	Medium	
on page 708.	Narrow	
Codice Fiscale	Wide	Digits Letters Only
See "Codice Fiscale data identifier" on page 712.		
Credit Card Magnetic Stripe Data	Medium	Digits Only
See "Credit Card Magnetic Stripe Data data identifier" on page 713.		
Credit Card Number	Wide	Digits Only
See "Credit Card Number data identifier" on page 715.	Medium	
	Narrow	
CUSIP Number	Wide	Lowercase
See "CUSIP Number data identifier" on page 726.	Medium	
	Narrow	

System data identifier breadths and normalizers (continued) Table 22-13

data identifier	Breadth(s)	Normalizer
Driver's License Number – CA State	Wide	Lowercase
See "Drivers License Number – CA State data identifier" on page 730.	Medium	
Driver's License Number – FL, MI, MN States	Wide	Lowercase
See "Drivers License Number - FL, MI, MN States data identifier" on page 732.	Medium	
Driver's License Number – IL State	Wide	Lowercase
See "Drivers License Number - IL State data identifier" on page 735.	Medium	
Driver's License Number – NJ State	Wide	Lowercase
See "Drivers License Number - NJ State data identifier" on page 737.	Medium	
Driver's License Number – NY State	Wide	Lowercase
See "Drivers License Number - NY State data identifier" on page 740.	Medium	
French INSEE Code	Wide	Digits Only
See "French INSEE Code data identifier" on page 742.		
Hong Kong ID	Wide	Lowercase
See "Hong Kong ID data identifier" on page 743.		
IBAN Central	Wide	None
See "IBAN Central data identifier" on page 743.		
IBAN East	Wide	None
See "IBAN East data identifier" on page 745.		
IBAN West	Wide	None
See "IBAN West data identifier" on page 748.		
IP Address	Wide	None
See "IP Address data identifier" on page 750.	Medium	
	Narrow	

System data identifier breadths and normalizers (continued) Table 22-13

data identifier	Breadth(s)	Normalizer
National Drug Code	Wide	None
See "National Drug Code (NDC) data identifier" on page 754.	Medium	
	Narrow	
People's Republic of China ID	Wide	Lowercase
See "People's Republic of China ID data identifier" on page 758.		
Randomized US Social Security Number (SSN)	Narrow	Digits Only
See "Randomized US Social Security Number (SSN) data identifier" on page 759.		
Singapore NRIC	Wide	Lowercase
See "Singapore NRIC data identifier" on page 760.		
South Korean Resident Registration Number	Wide	Digits Only
See "South Korea Resident Registration Number data identifier" on page 761.	Medium	
Spanish DNI ID	Wide	Lowercase
See "Spanish DNI ID data identifier" on page 763.		
SWIFT Code	Wide	Swift
See "SWIFT Code data identifier" on page 764.	Narrow	
Swiss AHV Number	Wide	Digits Only
See "Swiss AHV Number data identifier" on page 767.		
Taiwan ID	Wide	None
See "Taiwan ID data identifier" on page 767.		
UK Driver's License Number	Wide	Lowercase
See "UK Drivers License Number data identifier" on page 768.	Medium	
UK Electoral Roll Number	Wide	Lowercase
See "UK Electoral Roll Number data identifier" on page 772.		
UK National Health Service (NHS) Number	Medium	Digits Only
See "UK National Health Service (NHS) Number data identifier" on page 773.	Narrow	

data identifier	Breadth(s)	Normalizer
UK National Insurance Number	Wide	Lowercase
See "UK National Insurance Number data identifier"	Medium	
on page 777.	Narrow	
UK Passport Number	Wide	None
See "UK Passport Number data identifier" on page 781.	Medium	
	Narrow	
UK Tax ID Number	Wide	None
See "UK Tax ID Number data identifier" on page 785.	Medium	
	Narrow	
US Individual Tax ID Number (ITIN)	Wide	Digits Only
See "US Individual Tax Identification Number (ITIN) data	Medium	
identifier" on page 788.	Narrow	
US Social Security Number (SSN)	Wide	Digits Only
See "US Social Security Number (SSN) data identifier"	Medium	
on page 793.	Narrow	

Table 22-13 System data identifier breadths and normalizers (continued)

## Using optional validators

Table 22-14 lists the optional validators policy authors can configure for system data identifiers.

See "About optional validators for data identifiers" on page 547.

Table 22-14 Available optional validators for policy instances

Optional validator	Description	
Require beginning characters	Match the characters that begin (lead) the matched data item.	
Characters	For example, for the CA Drivers License data identifier, you could require the beginning character to be the letter "C." In this case the engine matches a license number C6457291.	
	See "Acceptable characters for optional validators" on page 560.	
Require ending characters	Match the characters that end (trail) the matched data item.	
	See "Acceptable characters for optional validators" on page 560.	

Optional validator	Description
Exclude beginning	Exclude from matching characters that begin (lead) the matched data.
characters	See "Acceptable characters for optional validators" on page 560.
Exclude ending	Exclude from matching the characters that end (trail) the matched data item.
characters	See "Acceptable characters for optional validators" on page 560.
Find keywords	Match one or more keywords or key phrases in addition to the matched data item.
	The keyword must be detected in the same message component as the data identifier content to repot a match.
	See "About cross-component matching" on page 548.
	This optional validator accepts any characters (numbers, letters, others).
	See "Acceptable characters for optional validators" on page 560.
	See "List of pattern validators that accept input data" on page 566.

Table 22-14 Available optional validators for policy instances (continued)

## Configuring optional validators

You implement optional validators to refine the scope of a data identifier defined in a policy instance. System and custom data identifiers support the configuration of optional validators.

See "About optional validators for data identifiers" on page 547.

The type of input allowed by an optional validator (numbers, letters, characters) depends on the data identifier. If you enter unacceptable input characters and attempt to save the configuration, the system reports an error.

For example, the US Social Security Number (SSN) data identifier accepts numbers only. If you configure the "Require ending character" optional validator and provide input as letters, you receive the following error when you attempt to save the configuration: Input to "Require ending characters" Validator is incorrect: List contains non-number character.

See Table 22-15 on page 560.

#### To configure an optional validator

- 1 Click the plus sign beside the **Optional Validators** label for the data identifier instance you are configuring.
  - See "Configuring the Content Matches data identifier condition" on page 552.
- Select one or more optional validators.
  - See "About optional validators for data identifiers" on page 547.
- 3 Provide the expected input for each optional validator you select. Each value can be of any length. Use commas to separate multiple values.
- 4 Click **Save** to save the configuration.

If the system displays an error message, make sure you have entered the correct type of expected character input.

See Table 22-15 on page 560.

## Acceptable characters for optional validators

Each optional validator requires you to enter in some data values. You must enter the appropriate type of data according for that data identifier. Table 22-15 lists the acceptable data type for each data identifier/optional validator pairing.

See "About optional validators for data identifiers" on page 547.

Note: The Find keyword optional validator accepts any characters as values for all data identifiers.

The type of data expected by the optional validator depends on the data identifier. Most data identifier/optional validator pairings accept numbers only; some accept alphanumeric values, and a few accept any characters. If you enter unacceptable input and attempt to save the policy, the system reports an error.

See "Configuring optional validators" on page 559.

**Table 22-15** Acceptable characters for optional validators

data identifier	Require ending characters	Exclude ending characters	Require beginning characters	Exclude beginning characters
US Social Security Number (SSN)		Num	nbers only	
Canadian Social Insurance Number		Num	nbers only	

Acceptable characters for optional validators (continued) **Table 22-15** 

data identifier	Require ending characters	Exclude ending characters	Require beginning characters	Exclude beginning characters
US Individual Tax Identification Number (ITIN)		Num	nbers only	
Driver's License Number – CA State	Numbe	ers only	Any characters (nor	malized to lowercase)
Driver's License Number – IL State	Numbe	ers only	Any characters (normalized to lowercase)	
Driver's License Number – NJ State	Numbe	ers only	Any characters (normalized to lowercase)	
Driver's License Number – NY State		Nun	nbers only	
Driver's License Number – FL, MI, MN States	Numbe	ers only	Any characters (nor	rmalized to lowercase)
Credit Card Number		Num	nbers only	
ABA Routing Number		Num	nbers only	
CUSIP Number	Numbers only			
SWIFT Code	Alphanumeric (numbers or letters)			
Credit Card Magnetic Stripe Data	Numbers only			
IBAN West	Alphanumeric (numbers or letters)			
IBAN Central	Alphanumeric (numbers or letters)			
IBAN East	Alphanumeric (numbers or letters)			
National Drug Code	Numbers only			
Australian Medicare Number		Num	nbers only	
IP Address		Any	characters	
Codice Fiscale	Numbers only			
Spanish DNI ID	Numbers only			
Burgerservicenummer	Numbers only			
UK Driver's License Number	Alphanumeric (normalized to lowercase)			
UK Tax ID Number	Numbers only			
UK Passport Number	Numbers only			

Table 22-13 Acceptable characters for optional validators (continued)				
data identifier	Require ending characters	Exclude ending characters	Require beginning characters	Exclude beginning characters
UK National Insurance Number		Alphanumeric (no	ormalized to lowerca	se)
UK National Health Service (NHS) Number	Numbers only			
UK Electoral Roll Number	Numbers only Any characters (normalized to lowercase		malized to lowercase)	
French INSEE Code	Numbers only			
Swiss AHV Number	Numbers only			
Australian Tax File Number	Numbers only			
People's Republic of China ID	Numbers only			
Hong Kong ID	Numbers only			
Singapore NRIC	Numbers only			
South Korean Resident Registration Number	Numbers only			
Taiwan ID	Numbers only			

Table 22-15 Acceptable characters for optional validators (continued)

## Using unique match counting

When you define a new data identifier rule, Count all unque matches is the default method for counting matches. As the name indicates,

The following table describes unique match counting characteristics.

Unique match counting characteristics **Table 22-16** 

Unique match counting characteristic	Description
First match is unique	A unique match is the first match found in a message component.  See "Detection messages and message components" on page 305.
Match count updated for each unique match	The match count is incremented by 1 for each unique pattern match.

Unique match counting characteristic	Description
Only unique matches are highlighted	Duplicate matches are neither counted nor highlighted at the Incident Snapshot screen
	See "Remediating incidents" on page 943.
Uniqueness does not span message components	For example, if the same SSN appears in both the message body and attachment, two unique matches will be generated, not one. This is because each instance is detected in a separate message component.
Compound rule with data identifier and keyword proximity conditions	In a compound rule combining a data identifier condition with a keyword condition that specifies keyword proximity logic, the reported match will not be the first match found, but the first match within the distance of the keyword proximity range.
No backward combatability	Unique match counting is only available for policies configured using version 11.6 or later Enforce Server. In addition, only version 11.6 or later Detection Servers and DLP Agents can run policies containing unique match counting.  See "Configuring unique match counting" on page 563.

Table 22-16 Unique match counting characteristics (continued)

## Configuring unique match counting

Count all unique matches is the default selection for new data identifiers you create. After upgrading Data Loss Prevention, you may need to manually configure pre-existing data identifier rules to use unique match counting, if you have not done so prior to upgrade

See "About unique match counting" on page 549.

#### To configure unique match counting

- 1 Select the policy containing the data identifier rule or rules you want to update at the Manage > Policies > Policy List screen.
- 2 Select the data identifier rule at the **Configure Policy** screen.
- 3 Select the match counting option **Count all unique matches**.
- 4 Click **OK** to apply the unique match counting configuration change.

- 5 Click **Save** to save the policy change.
- 6 Test unique match counting.

Create an incident with multiple instances of a data identifier pattern, such as several instances of the same social security number in the same message component (for example, in an email attachment).

At the Incident Snapshot verify that only unique matches are highlighted and counted.

# Modifying system data identifiers

The system lets you modify system-defined data identifiers, but you cannot delete them. Any modifications you make to the configuration of a system-defined data identifier take effect system-wide. This means that the modifications apply to any policies that actively or subsequently declare the Data identifier.

There is no way to automatically revert a data identifier to its original configuration once it is modified. Before you modify a system data identifier, consider cloning it.

, and any custom data identifiers that you have created. Any modification you make to a Data identifier takes effect system wide. This means the modifications apply to any policy that declares the modified Data identifier.

The system does not include modified data identifiers in policies exported as templates. Before modifying a system data identifier, export any policies that declare it.

See "Editing data identifiers" on page 551.

See "Editing pattern validator input" on page 566.

Note: The system does not export modified and custom data identifiers in a policy template. The system exports a reference to the system Data identifier. The target system where the policy template is imported provides the actual Data identifier. See "Clone system-defined data identifiers before modifying to preserve original state" on page 581.

See "Editing data identifiers" on page 551.

System Data identifier modification options Table 22-17

Modifiable at the system level	Not configurable
<ul> <li>Patterns         You can edit one or more Data identifier patterns at the system level.</li> <li>Active Validators         You can add or remove required validators at the system level.</li> <li>Data Entry         You can edit the input of an active validator for a system Data identifier.</li> </ul>	<ul> <li>Name, Description, and Category         You cannot modify the name, description, or category of         a system Data identifier.</li> <li>Breadth         You cannot define a new detection breadth for a system         Data identifier; you can only modify an existing breadth.</li> <li>Optional Validators         You cannot define optional validators at the system level.         You can only configure optional validators at the policy         level.</li> <li>Data Normalizer         You cannot modify the type of data normalizer         implemented by a system Data identifier.</li> <li>Delete         You cannot delete a system Data identifier.</li> </ul>

## Cloning a system data identifier before modifying it

The Enforce Server does not provide an automated mechanism for cloning a system Data Identifier.

See "Extending and customizing data identifiers" on page 546.

Before you modify a system Data Identifier, consider manually cloning it so you can revert to the original configuration, if necessary. At the least, you should export a policy as a template before you modify any system Data Identifier declared by that policy.

#### To manually clone a system Data Identifier

- Review the original configuration of the Data Identifier you want to modify.
- 2 Create a custom Data Identifier.
  - See "Workflow for creating custom data identifiers" on page 570.
- Copy the configuration of the original Data Identifier to the custom Data 3 Identifier.
  - Add the pattern(s), validator(s), any data input, and the normalizer.
  - See "Selecting a data identifier breadth" on page 555.
- 4 Save the custom Data Identifier.
- 5 Modify the custom Data Identifier to suit your needs.

## Editing pattern validator input

At the system-level you can edit the data input that a required validator accepts. Not all validators accept data input.

See "About pattern validators" on page 548.

#### To edit required validator input

- Edit the data identifier by selecting it from the Manage > Policies > data identifiers screen.
- Select the Rule Breadth you want to modify.
  - Generally, the medium and narrow breadth options include validators that accept data input.
- 3 Select the editable validator from the **Active Validators** list whose input you want to edit.

For example, select Find keywords.

See "List of pattern validators that accept input data" on page 566.

- 4 Edit the input for the validator in the **Description and Data Entry** field.
- Click **Update Validator** to save the changes you have made to the validator input.
  - Click **Discard Changes** to not save the changes.
- Click **Save** to save the data identifier.

## List of pattern validators that accept input data

The following table lists all available pattern validators that require data input. The input data is editable at the system-level definition of the data identifier.

Note: Input you use for beginning and ending validators concern the text of the match itself. Input you use for prefix and suffix validators concern characters before and after matched text.

**Table 22-18** Pattern validators that accept input data

Validator	Description
Exact Match	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
Exclude beginning characters	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.

Validator	Description
Exclude ending characters	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
Exclude exact match	Enter a comma-separated list of values. Each value can be of any length.
Exclude prefix	Enter a comma-separated list of values. Each value can be of any length.
Exclude suffix	Enter a comma-separated list of values. Each value can be of any length.
Find keywords	Enter a comma-separated list of values. Each value can be of any length.
Require beginning characters	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
Require ending characters	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.

Table 22-18 Pattern validators that accept input data (continued)

## Editing keywords for international PII data identifiers

Data identifiers offer broad support for detecting international content.

See "Introducing data identifiers" on page 541.

Some international data identifiers offer a wide breadth of detection only. In this case you can implement the Find Keywords optional validator to narrow the scope of detection. Implementing this optional validator may help you eliminate any false positives that your policy matches.

See "Selecting a data identifier breadth" on page 555.

#### To use keywords for international data identifiers

- Create a policy using one of the system-provided international data identifiers 1 that is listed in the table.
  - See "List of keywords for international system data identifiers" on page 568.
- 2 Select the **Find Keywords** optional validator.
  - See "Configuring the Content Matches data identifier condition" on page 552.
- 3 Copy and past the appropriate comma-separated keywords from the list to the Find Keywords optional validator field.
  - See "Configuring optional validators" on page 559.

## List of keywords for international system data identifiers

See Table 22-19 on page 568. provides keywords for several system-defined international data identifiers. You can modify the specified data identifier using the corresponding keyword(s).

See "Extending and customizing data identifiers" on page 546.

See "Introducing data identifiers" on page 541.

See "Selecting a data identifier breadth" on page 555.

Table 22-19 Keyword list for international PII data identifiers

Data identifier	Language	Keywords	English translation
Burgerservicenummer (BSN)	Dutch	Persoonsnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden	person number, social-fiscal number (abbreviation), social-fiscal number, person-related number
Codice Fiscale	Italian	codice fiscal, dati anagrafici, partita I.V.A., p. iva	tax code, personal data, VAT number, VAT number
French INSEE Code	French	INSEE, numéro de sécu, code sécu	INSEE, social security number, social security code
Hong Kong ID	Chinese (Traditional)	身份證,三顆星	Identity card, Hong Kong permanent resident ID Card
International Bank Account Number (IBAN) Central	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
International Bank Account Number (IBAN) East	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
International Bank Account Number (IBAN) West	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
People's Republic of China ID	Chinese (Simplified)	身份证,居民信息,居民身份信息	Identity Card, Information of resident, Information of resident identification
South Korea Resident Registration Number	Korean	주민등록번호, 주민번호	Resident Registration Number, Resident Number
Spanish DNI ID	Spanish	DNI	DNI

Data identifier	Language	Keywords	English translation
Swiss AHV Number	French	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité soclale, Numéro AVH	AVS number, insurance number, national identifier, national insurance number, social security number, AVH number
	German	AHV-Nummer, Matrikelnumme, Personenidentifikationsnummer	AHV number, Swiss Registration number, PIN
	Italian	AVS, AVH	AVS, AVH
Taiwan ID	Chinese (Traditional)	中華民國國民身分證	Taiwan ID

Keyword list for international PII data identifiers (continued) Table 22-19

## Updating policies to use the Randomized US SSN data identifier

The Randomized US Social Security Number (SSN) data identifier detects both traditional and randomized SSNs.

See "Use the Randomized US SSN data identifier to detect SSNs" on page 582.

All policy templates that previously used the US Social Security Number (SSN) data identifier to detect SSNs are updated to use the Randomized US Social Security Number (SSN) data identifier. In addition, the Randomized US SSN data identifier is updated for Symantec Data Loss Prevention version 12.5.

See "Updating policies after upgrading to the latest version" on page 355.

If you have existing policies that use the US SSN data identifier to detect SSNs, you should update each policy to use the Randomized US SSN data identifier. If you have created policies using the version 12.0 Randomized US SSN data identifier. you should update each to use the version 12.5 Randomized US SSN data identifier.

To update a policy to use the Randomized US SSN data identifier provides steps for updating your SSN policies.

#### To update a policy to use the Randomized US SSN data identifier

- Edit the policy that implements the US SSN data identifier or the 12.0 Randomized US SSN data identifier.
  - See "Configuring policies" on page 326.
- Edit the rule that contains the US SSN data identifier.
  - See "Configuring policy rules" on page 330.
- 3 Remove the US SSN data identifier.

- 4 Add the Randomized US SSN data identifier.
  - See "Managing and adding data identifiers" on page 550.
- 5 Save the policy.
- Test policy detection for both traditional and randomized US SSNs. See "Test and tune policies to improve match accuracy" on page 361.
- 7 Deploy the updated SSN policy into production. See "Policy deployment" on page 288.

# **Creating custom data identifiers**

You can create and delete one or more custom data identifiers. A custom data identifier may be a system data identifier that you have cloned and intend to modify, or one that you create from scratch. A custom data identifier is reusable across policies. Changes made to a custom data identifier at the system-level affect any policies that actively or subsequently declare the custom data identifier.

Table 22-20 lists the components of custom data identifiers.

See "Workflow for creating custom data identifiers" on page 570.

Table 22-20 Custom data identifier components

Component	Description
Patterns	Define one or more regular expression patterns, separated by line breaks.  See "About data identifier patterns" on page 547.
Validators	Add or remove validators to perform validation checks on the data detected by the pattern(s).  See "About pattern validators" on page 548.
Data Entry	Provide comma-separated data values for any validators that require data input.  See "About pattern validators" on page 548.
Normalizer	Select a normalizer to standardize the data before matching against it.  See "Selecting a data normalizer" on page 578.

## Workflow for creating custom data identifiers

You can implement custom data identifiers to detect unique content. To implement a custom data identifier, you must define at least one pattern and select a data normalizer. Validators are optional.

See "Custom data identifier configuration" on page 572.

When you define a custom data identifier, the system assigns it to the "Wide" breadth by default. This is not a limitation, however, because the actual scope of detection is determined by the pattern(s) and validator(s) that you define.

Implementing custom data identifiers Table 22-21

Step	Action	Description
Step 1	Select Manage > Policies > data identifiers.	The data identifiers screen lists all data identifiers available in the system.
Step 2	Select Add data identifier.	Enter a <b>Name</b> for the custom data identifier.  The name must be unique.  Enter a <b>Description</b> for the custom data identifier.  A custom data identifier is assigned to the <b>Custom</b> category by default and cannot be changed.
		The description field is limited to 255 characters per line.
Step 3	Enter one or more <b>Patterns</b> to match data.	You must enter at least one pattern for the custom data identifier to be valid.  Separate multiple patterns by line breaks.  See "Writing data identifier patterns to match data" on page 574.
Step 4	Select a Data Normalizer.	You must select a data normalizer.  See "Selecting a data normalizer" on page 578.  The following normalizers are available:  Digits  Digits and Letters  Lowercase  Swift codes  Do nothing Select this option if you do not want to normalize the data.
Step 5	Select zero or more Validators.	Including a validator to check and verify pattern matching is optional.  See "Selecting pattern validators" on page 577.

Step	Action	Description
Step 6 Save the custom data identifier.		Click <b>Save</b> at the upper left of the screen.
	Once you define and save a custom data identifier, it appears alphabetically in the list of data identifiers at the <b>data identifiers</b> screen.	
		To edit a custom data identifier, select it from the list.
	See "Editing data identifiers" on page 551.	
		Note: Click Cancel to not save the custom data identifier.
Step 7 Implement the custom data identifier in one or more policies.	The system lists all custom data identifiers beneath the <b>Custom</b> category for the "Content Matches data identifier" condition at the <b>Configure Policy</b> - Add Rule and the <b>Configure Policy</b> - Add Exception screens.	
		See "Configuring the Content Matches data identifier condition" on page 552.
		You can configure optional validators at the policy instance level for custom data identifiers.
		See "Configuring optional validators" on page 559.

Table 22-21 Implementing custom data identifiers (continued)

# Custom data identifier configuration

You can create and delete one or more custom data identifiers . A custom Data identifier can be used across policies. Changes made to a custom Data identifier at the system-level affect any policies that actively or subsequently declare the custom Data identifier.

See "Workflow for creating custom data identifiers" on page 570.

Table 22-22 Custom data identifier configuration

Configurable at the custom level	Not configurable
<ul> <li>Name and Description         You must give a custom Data identifier a unique name.         It is good practice to provide a description for the custom Data identifier.         You can change the name or description of a custom Data identifier when you modify it.         Patterns         You must define at least one pattern for the custom Data identifier to be valid.         Active Validators         You can add one or more required validators to a custom Data identifier.         Data Entry         You can edit the input of an active validator that accepts data input.         Data Normalizer         You must select a data normalizer when defining a custom Data identifier.</li> </ul>	Optional Validators     Custom data identifiers support all optional validators, but they are configured at the policy instance level.

## Using the data identifier pattern language

The Data identifier pattern language is a limited subset of the regular expression lexicon. The Data identifier pattern language does not support all of the regular expressions characters and constructs. A regular expression pattern converted to a Data identifier pattern will require some syntactical modifications.

Data identifier patterns are limited to 100 characters per line. The pattern itself can be more than 100 characters, but a line cannot have more than 100 character. You should split the pattern up by lines not longer than 100 characters.

See "Input character limits for policy configuration" on page 344.

The table below lists the known differences between regular expressions and the Data identifier pattern language.

Character	Description
*	The asterisk (*), pipe ( ), and dot (.) characters are not supported for Data identifier
	patterns.
•	
\w	The \w construct cannot be used to match the underscore character (_).
\s	The \s construct cannot be used to match a whitespace character; instead, use an actual whitespace.
\d	For digits, use the construct \d.
Grouping	Grouping only works at the beginning of the pattern, for example:
	\d{4} - 2049 does not work; instead use 2049 - \d{4}
	\d{2} /19 \d{2} does not work; instead use \d{2} /[1][9] \d{2}
	Groupings are allowed at the beginning of the pattern, like in the credit card Data identifier.

Table 22-23 Data identifier pattern language limitations

## Writing data identifier patterns to match data

If you modify an existing data identifier, you can edit its patterns. If you create a custom data identifier, you must implement at least one pattern. Data identifier patterns are implemented using a syntax that is similar to the regular expression language, with limitations. In addition, the system only allows the use of ASCII characters for data identifier patterns.

See "About data identifier patterns" on page 547.

#### To edit or implement a pattern

- Review the patterns for the data identifier you want to modify. See "Selecting a data identifier breadth" on page 555.
- 2 Consider cloning the data identifier, if you are modifying a system data identifier. See "Cloning a system data identifier before modifying it" on page 565.
- 3 Select Manage > Policies > data identifiers in the Enforce Server administration console.
- 4 Select the data identifier you want to modify.
- 5 Select the breadth for the data identifier you want to modify. Generally, patterns vary among detection breadths.

6 In the **Patterns** field, modify an existing pattern, or enter one or more new patterns, separated by line breaks.

Data identifier patterns are implemented as regular expressions. However, much of the regular expression syntax is not supported.

See "Using the data identifier pattern language" on page 573.

7 Click **Save** to save the data identifier.

## Using pattern validators

The following table lists all available pattern validators. Validators marked with an asterisk (\*) beside the name in the table below require data input.

Available validators for system and custom data identifiers Table 22-24

Validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted check sum.
Advanced KRRN Validation	Validates that 3rd and 4th digit are a valid month, that 5th and 6th digit a valid day, and the checksum matches the check digit.
Advanced SSN	Validator checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
Australian Tax File validation check	Computes the checksum and validates the pattern against it.
Basic SSN	Performs minimal SSN validation.
Burgerservicenummer Check	Performs a check for the Burgerservicenummer.
China ID checksum validator	Computes the checksum and validates the pattern against it.
Codice Fiscale Control Key Check	Computes the control key and checks if it is valid.
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).
Custom Script*	Enter a custom script to validate pattern matches for this Data identifier breadth.  See "Creating custom script validators" on page 579.
DNI control key check	Computes the control key and checks if it is valid.

Available validators for system and custom data identifiers *(continued)* **Table 22-24** 

Validator	Description
Duplicate digits	Ensures that a string of digits are not all the same.
Exact Match*	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
Exclude beginning characters*	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
	<b>Note:</b> Beginning and ending validators concern the text of the match itself. Prefix and suffix validators concern characters before and after matched text.
Exclude ending characters*	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.
Exclude exact match*	Enter a comma-separated list of values. Each value can be of any length.
Exclude prefix*	Enter a comma-separated list of values. Each value can be of any length.
	<b>Note:</b> Prefix and suffix validators concern characters before and after matched text. Beginning and ending validators concern the text of the match itself.
Exclude suffix*	Enter a comma-separated list of values. Each value can be of any length.
Find keywords*	Enter a comma-separated list of values. Each value can be of any length.
Hong Kong ID	Computes the checksum and validates the pattern against it.
INSEE Control Key	Validator computes the INSEE control key and compares it to the last 2 digits of the pattern.
IP Basic Check	Every IP address must match the format x.x.x.x and every number must be less than 256.
IP Octet Check	Every IP address must match the format x.x.x.x, every number must be less than 256, and no IP address can contain only single-digit numbers (1.1.1.2).
IP Reserved Range Check	Checks whether the IP address falls into any of the "Bogons" ranges. If so the match is invalid.
Luhn check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.
No Validation	Performs no validation.
Number Delimiter	Validates a match by checking the surrounding digits.

Available validators for system and custom data identifiers Table 22-24 (continued)

Validator	Description	
Require beginning characters*	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.	
Require ending characters*	Enter a comma-separated list of values. If the values are numeric, do NOT enter any dashes or other separators. Each value can be of any length.	
Singapore NRIC	Computes the Singapore NRIC checksum and validates the pattern against it.	
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.	
Swiss AHV	Swiss AHV Modulus 11 Checksum.	
Taiwan ID	Taiwan ID checksum.	
UK Drivers License	Every UK drivers license must be 16 characters and the number at the 8th and 9 position must be larger than 00 and smaller than 32.	
UK NHS	UK NHS checksum.	

#### Selecting pattern validators

Symantec Data Loss Prevention provides a comprehensive set of validators to facilitate pattern matching accuracy.

See "About pattern validators" on page 548.

When you modify a data identifier, the system exposes the active validators used by the data identifier. When you modify or create a data identifier, the system displays all system-defined data validators from which you can choose.

Note: The active validators that allow for and define input are not to be confused with the "Optional validators" that can be configured for any runtime instance of a particular data identifier. Optional validators are always configurable at the instance level. Active validators are only configurable at the system level.

Select a validator from the "Validation Checks" list on the left, then click Add Validator to the right. If the validator requires input, provide the required data using a comma-separated list and then click Add Validator.

See "Selecting pattern validators" on page 577.

#### To select a pattern validator

Create a custom data identifier.

See "Workflow for creating custom data identifiers" on page 570.

2 In the **Validators** section, select the desired validator.

See "About pattern validators" on page 548.

3 If the validator does not require data input, click Add Validator.

The validator is added to the Active Validators list.

If the validator requires data input, enter the data values in the **Description** and Data Entry field.

Click **Add Validator** when you are done entering the values.

The validator is added to the **Active Validators** list.

- 5 To remove a validator, select it in the **Active Validators** list and click the red X icon.
- Click **Save** to save the configuration of the data identifier.

#### Selecting a data normalizer

When you create a custom Data identifier, you must select a normalizer to reconcile the data detected by the pattern with the format expected by the validators.

See "Workflow for creating custom data identifiers" on page 570.

Table 22-25 lists and describes the normalizers you can implement for custom data identifiers .

Note: You cannot modify the normalizer of a system-defined Data identifier.

Available data normalizers Table 22-25

Normalizer	Description
Digits	Only numeric characters are allowed.
Digits and Letters	Alphanumeric characters are allowed.
Lowercase	Only letters are allowed, normalized to lowercase.
Swift codes	Code must match SWIFT requirements.
Do nothing	The data is not normalized, evaluated as entered by the user.

#### Creating custom script validators

The custom script validation check lets you enter a custom script to validate pattern matches. To implement a custom validator, you use the Symantec Data Loss Prevention Scripting Language.

You can implement a custom script validator in a system data identifier you modify or in a custom data identifier.

Note: Refer to the Symantec Data Loss Prevention Detection Customziation Guide for details on using the Symantec Data Loss Prevention Scripting Language.

#### To implement a custom script validator

- Modify an existing data identifier or create a custom data identifier. See "Workflow for creating custom data identifiers" on page 570.
- 2 Select the **Custom Script** validator from the list of **Validation Checks**.
- 3 Enter your custom script in the **Description and Data Entry** field.
- Click Add Validator to add the custom validator to the Active Validators list.
- 5 Click **Save** to save the configuration of the data identifier.

## Best practices for using data identifiers

Data identifiers are algorithms that combine pattern matching with data validators to detect content. Symantec Data Loss Prevention provides a number of system-defined data identifiers for common data patterns, including SSNs, Tax IDs, and more. In addition, you can define your own custom data identifiers to match any data you can describe using the data identifier pattern language. Data identifiers are commonly used to detect personally identifiable information (PII).

This section provides best practices for implementing data identifier policies.

Table 22-26 summarizes the best practices in this section.

Table 22-26 Summary of data identifier best practices

Best practice	Description
Use data identifiers instead of regular epressions when possible.	See "Use data identifiers instead of regular expressions to improve accuracy" on page 580.
Modify data identifier definitions when you want tuning to apply globaly.	See "Modify data identifier definitions when you want tuning to apply globally" on page 581.

Best practice	Description
Close system-defined data identifiers before modifying them.	See "Clone system-defined data identifiers before modifying to preserve original state" on page 581.
Consider using multiple data identifer breadth in parallel	See "Consider using multiple breadths in parallel to detect different severities of confidential data" on page 582.
Avoid matching on the Envelope over HTTP	See "Avoid matching on the Envelope over HTTP to reduce false positives" on page 582.
Use the Randomized US SSN data identifier to detect traditional and randomized SSNs	See "Use the Randomized US SSN data identifier to detect SSNs" on page 582.
Use unique match counting to improve accuracy and ease remediation	See "Use unique match counting to improve accuracy and ease remediation" on page 583.

Summary of data identifier best practices (continued) Table 22-26

#### Use data identifiers instead of regular expressions to improve accuracy

Data identifiers are designed to protect personally identifiable information (PII) with very good accuracy (<10% false positive rate). If a data identifier is available for the type of content you want to protect, you should use the data identifier instead of a regular expression because data identifiers are more efficient than regular expressions. Out-of-the-box data identifier patterns are tuned for accuracy, including region, industry, and country nuances. In addition, data identifiers include validation checks to verify the data matched by the pattern. This additional layer of intelligence screens out test data and other triggers of false positive incidents. Regular expressions, on the other hand, can be computationally expensive and can lead to increased false positives.

For example, if you want to detect social security numbers (SSN), you would use the Randomized US SSN data identifier instead of a regular expression pattern. The Randomized US SSN data identifier is more accurate than any regular expression you could write and much easier and guicker to implement.

**Note:** The data identifier pattern language is a limited subset of the regular expression language. Not all regular expression constructs or characters are supported for data identifier patterns. See "Using the data identifier pattern language" on page 573.

#### Clone system-defined data identifiers before modifying to preserve original state

Before you modify a system data identifier or create a custom data identifier, consider the following:

- If you want to modify a system data identifier, manually clone it as a custom data identifier and then modify the cloned copy. In this fashion you preserve the state of the original system-defined data identifier.
- Data identifiers do not export as part of a policy template. As such, you should add the data identifier to a policy and export the policy as a template before modifying the data identifier.

An exported template contains a reference to each data identifier implemented in that policy. On import to a target system, the template uses a reference to select the local data identifier. If the system data identifier is modified, on import it cannot be recognized by the target system.

See "Cloning a system data identifier before modifying it" on page 565.

#### Modify data identifier definitions when you want tuning to apply globally

Data identifiers offer two levels of configuration:

- Definitions
- Instances

Data identifier definitions are configured at the system-level of the Enforce Server. At the definition level you can tune the data supplied by any required validator that the definition declares at this level, as well as what validators are used.

Data identifier instances can only configured at the policy rule level. Any configurations made at the rule level are local in scope and applicable only to that policy. At the rule level you use optional validators, such as require or exclude beginning or ending characters, to tune the instance of the data identifier rule.

The general recommendation is to configure data identifier definitions so that the changes apply globally to any instance of that data identifier definition. Such configurations are reusable across policies. Rule-level optional validators, such as, should be used for unique policies.

#### Consider using multiple breadths in parallel to detect different severities of confidential data

Matching data identifiers against content often requires fine-tuning as you adjust the configuration to keep both false positives and false negatives to a minimum. After you configure an instance of the Content Matches Data Identifier condition, study the matches and adjust the configuration to ensure optimum data matching success.

Consider adjusting the data identifier breadth you are using if the data identifier is producing too many false positive or negatives. For example, if you are using a wide breadth and receiving many false positives, consider using a medium or narrow breadth.

See "About data identifier breadths" on page 547.

As an alternative approach, consider using multiple data identifier breadths in parallel in the same rule with different severity levels for each rule. For example, in a single policy designed to detect credit card numbers, you could add three rules to the policy, each using a different breadth (one wide, one medium, one narrow). You would then set the severity for the narrow to be high severity incidents, and the wide to be low severity incidents. Using this layered approach lets you survey the data flowing through the enterprise using a policy that covers both ends of spectrum. You can use this sampling-based approach to focus your remediation efforts on the highest-priority incidents while still detecting and being able to review low-severity incidents.

#### Avoid matching on the Envelope over HTTP to reduce false positives

Sometimes HTTP transmissions contain session IDs in the header that can trigger false positives for numeric data identifiers. For example, some social media sites such as Facebook and LinkedIn contain a session ID that may at times match the CCN and SSN data identifiers exactly, causing false positives.

To reduce false positives in connection with HTTP session IDs in the message header, the best practice is not to match on the "Envelope" message component when implementing numeric data identifiers, specifically the CCN or SSN data identifiers.

#### Use the Randomized US SSN data identifier to detect SSNs

In 2011, the United States Social Security Administration (SSA) began issuing randomized SSNs. Under this scheme, the high group number (second part of the SSN) no longer corresponds to the area number (first part of the SSN). Also, the range of the area number can go up to 899 instead of 773. Randomization applies to SSNs issued on or after June 25, 2011. It does not apply to SSNs issued before that date.

To support the new randomized SSN scheme, Symantec Data Loss Prevention provides the system-defined Randomized US Social Security Number (SSN) data identifier.

See "Randomized US Social Security Number (SSN) data identifier" on page 759.

The Randomized US SSN data identifier detects both traditional and randomized SSNs. The Randomized US SSN data identifier replaces the US SSN data identifier. which only detects traditional SSNs. In addition, the patterns for the Randomized US SSN data identifier are updated for version 12.5.

Symantec recommends that you use the Randomized US SSN data identifier for all new policies that you want to use to detect SSNs, and that you update your existing SSN policies to use the Randomized US SSN data identifier. For your existing policies that already implement the traditional US SSN data identifier, you can add the Randomized US SSN data identifier as an OR'd rule so that both run in parallel as you test the policy to ensure it accurately detects both styles of SSNs.

See "Updating policies to use the Randomized US SSN data identifier" on page 569.

#### Use unique match counting to improve accuracy and ease remediation

The data identifier rule configuration contains an option to count only unique matches. With this option selected (as opposed to the default setting which counts all matches), only unique matches will be reported as the first match found in the message or message component. Only unique matches are counted and highlighted.

The best practice is to use unique match counting when you only care about unique matches, not duplicate matches. For example, if you are using the Credit Card Numbers data identifier to protect credit card numbers, and you only care if a document contains 25 or more unique numbers, you would use the count all unique matches option instead of the count all matches option. If you counted all matches, a document containing 25 of the same CCNs would trigger the policy, which is not the objective of your policy.

See "About unique match counting" on page 549.

# Detecting content using keyword matching

This chapter includes the following topics:

- Introducing keyword matching
- Configuring keyword matching
- Best practices for using keyword matching

# Introducing keyword matching

Symantec Data Loss Prevention provides the **Content Matches Keyword** policy condition for keyword detection.

To detect data loss using keyword matching, the detection engine compares inbound messages or message components against each keyword in a list of one or more keywords or keyword phrases. Keyword matching supports both whole word and partial word matching, as well as word proximity. Keyword matching is supported on the server and on the endpoint.

Table 23-1 lists typical keyword matching use cases.

Configuration	Typical use	
Whole word matching	Languages based on the Latin alphabet	
	UTF-8 characters	
	Chinese, Japanese, and Korean (CJK) languages with token verification enabled for the server	
	CJK keywords on the endpoint	
	See "About keyword matching for Chinese, Japanese, and Korean (CJK) languages" on page 585.	
Partial word matching	Languages based on the Latin alphabet	
	Mixed languages	
	See "Keyword matching examples" on page 587.	

**Table 23-1** Keyword matching use cases

#### About keyword matching for Chinese, Japanese, and Korean (CJK) languages

Symantec Data Loss Prevention version 12.5 detection servers support natural language processing for Chinese, Japanese, and Korean (CJK) keywords. When natural language processing for CJK languages is enabled, the detection server validates CJK tokens before reporting a match. For CJK languages, a token is a single character which constitutes a word. Thus, partial word matching does not apply to CJK languages.

Token validation for CJK keywords is only supported for detection servers and is disabled by default. You must enable token validation for each detection server. In addition you must match on whole words for token validation to apply.

On the endpoint you can use whole word matching for CJK keywords.

Table 23-2 summarizes keyword matching use cases for CJK languages.

**Table 23-2** Keyword matching use cases for CJK languages

<b>Detection component</b>	Use case
Server	Enable token verification on the detection server and use whole word matching  See "Enabling and using CJK token verification for server keyword matching" on page 593.
Endpoint	Use whole word matching See "Keyword matching examples for CJK languages" on page 588.

#### About keyword proximity

Using keyword proximity, a policy author can define a pair of keywords and specify a word range between them. If the words occur within that range, a match is triggered. For example, an instance of the Content Matches Keyword condition might require that any instance of the words "confidential" and "information" occurring within 10 words of each other triggers a match.

Alternatively, you can use keyword proximity to exclude matching words within a specified distance by using the Content Matches Keyword condition as a detection exception. In this case any occurrence of the words "confidential" and "information" within 10 words of each is excepted from matching.

For Chinese, Japanese, and Korean (CJK) languages, a single CJK character is counted as one word.

See "Keyword matching syntax" on page 586.

See "Keyword matching examples" on page 587.

See "Configuring the Content Matches Keyword condition" on page 591.

#### Keyword matching syntax

When you define a keyword rule, the system evaluates every keyword in the condition list against each message component (header, subject, body, attachment).

Consider the following syntactical guidelines when creating keyword lists.

**Table 23-3** Keyword matching syntax

Behavior	Description	
Whole word matching	With whole word matching, keywords match at word boundaries only (\W in the regular expression lexicon). Any characters other than A-Z, a-z, and 0-9 are interpreted as word boundaries.	
	With whole word matching, keywords must have at least one alphanumeric character (a letter or a number). A keyword consisting of only white-space characters, such as "", is ignored.	
Quotation marks	Do not use quotation marks when you enter keywords or phrases because quotes are interpreted literally and will be required in the match.	
White space	The systems strips out the white space before and after keywords or key phrases. Each whitespace within a keyword phrase is counted.	
Case sensitivity	The case sensitivity option that you choose applies to all keywords in the list for that condition.	

**Table 23-3** Keyword matching syntax (continued)

Behavior	Description		
Plurals and verb inflections	All plurals and verb inflections must be specifically listed. If the number of enumerations becomes complicated use the wildcard character (asterisk [*]) to detect a keyword suffix (in whole word mode only).		
Keyword phrases	You can enter keyword phrases, such as <b>social security number</b> (without quotes). The system looks for the entire phrase without returning matches on individual constituent words (such as <b>social</b> or <b>security</b> ).		
Keyword variants	The system only detects the exact keyword or key phrase, not variants. For example, if you specify the key phrase <b>social security number</b> , detection does not match a phrase that contains two spaces between the words.		
Matching multiple keywords	The system implies an OR between keywords. That is, a message component matches if it contains any of the keywords, not necessarily all of them. To perform an ALL (or AND) keyword match, combine multiple keyword conditions in a compound rule or exception.		
Alpha-numeric characters	During keyword matching, only a letter or a digit is considered a valid keyword start position. Special characters (non-alphanumeric) are treated as delimiters (ignored). For example, the ampersand character ("&") and the underscore character ("_") are special characters and are not considered for keyword start position.		
	For example, consider the following:		
	keyword		
	Keyword		
	&&akeyword&&		
	123Keyword		
	For these examples, the valid keyword start positions are as follows: $k$ , $K$ , $a$ , and $1$ .		
	Note: This same behavior applies to keyword validators implemented in data identifiers.		
Proximity	The word distance (proximity value) is exclusive of detected keywords. Thus, a word distance of 10 allows for a proximity window of 12 words.		

### Keyword matching examples

To implement keyword matching, you can enter one or more keywords or phrases, each separated by a comma or newline character. You can match on whole or partial words, and specify case sensitivity. You can use the asterisk (\*) wildcard character to detect a keyword suffix (in whole word mode only).

See "Keyword matching syntax" on page 586.

Table 23-4 Keyword matching examples

Keyword type	Keyword(s)		Matches	<b>Does Not Match</b>
keyword	confidential		confidential -confidential; ®"confidential" ®Confidential ®CONFIDENTIAL	confidentially (in whole word mode only, otherwise it would match)
key phrase	internal use only		internal use only internal use ONLY (if case insensitive is selected)	internal use
keyword list keyword with wildcard	Newline delimited: hack hacker hacks priv*	Comma delimited: hack, hacker, hacks	hacks hack hacker  private privilege privy privity	hackers shack  prize prevent
La consul distingui			privs priv	
keyword dictionary	account number, account ps, american express, americanexpress, amex, bank card, bankcard, card num, card number, cc #, cc#, ccn, check card, checkcard, credit card, credit card #, credit card number, credit card#, debit card, debitcard, diners club, dinersclub, discover, enroute, japanese card bureau, jcb, mastercard, mc, visa, (etc)		If any keyword or phrase is present, the data is matched: amex credit card mastercard	amx creditcard master card car

# Keyword matching examples for CJK languages

Table 23-5 provides keyword matching examples for Chinese, Japanese, and Korean languages. All examples assume that the keyword condition is configured to match on whole words only.

If token verification is enabled, the message size must be sufficient for the token validator to recognize the language. For example: the message "東京都市部の人 □" is too small fo a message for the token validation process to recognize the language of the message. The following message is a sufficient size for token validation processing:

今朝のニュースによると東京都市部の人口は増加傾向にあるとのことでした。 全 国的な人口減少の傾向の中、東京への一極集中を表しています。

See "About keyword matching for Chinese, Japanese, and Korean (CJK) languages" on page 585.

Token validation for CJK language keywords is not available on the endpoint. To match CJK on the endpoint, you configure the condition to match on whole words only.

		-	-	
Language	Keyword	Matches on server with token validation ON	Matches on server with token validation OFF	Matches on endpoint
Chinese	通信	数字无线通信	数字无线通信 交通信息 网站	数字无线通信 交通信息网 站
Japanese	京都市	京都府京都市左京区	京都府京都市左京区 東 京都市部の人口	京都府京都市左京区東京 都市部の人
Korean	정부	정부의 방침	정부의 방침 의정부 경전 철	정부의 방침 의정부 경전 철

**Table 23-5** Keyword matching examples for CJK

#### About updates to the Drug, Disease, and Treatment keyword lists

The Drug, Disease, and Treatment keyword lists are updated with current terminology (as of 2013-12-09) based on information from the U.S. Federal Drug Administration (FDA) and other sources. The Drug, and Disease, and Treatment keyword lists are used by the HIPAA and HITECH (including PHI) and Caldicott Report policy templates.

When you upgrade your Data Loss Prevention system, the generic, system-defined HIPAA and Caldicott policy templates are updated with the recent Drug, Disease, and Treatment keyword lists. However, policies you have created based on the HIPAA or Caldicott policy templates are not automatically updated. This behavior is expected so that any changes or customizations you have made to your HIPAA or Caldicott policy templates are not overwritten by updates to the system-defined templates. Updating the Drug, Disease, and Treatment keyword lists for your HIPAA

and Caldicott policy templates is a manual process that you should perform to ensure your HIPAA or Caldicott policies are up to date.

See "Updating the Drug, Disease, and Treatment keyword lists for your HIPAA and Caldicott policies" on page 594.

See "Keep the keyword lists for your HIPAA and Caldicott policies up to date" on page 596.

See "HIPAA and HITECH (including PHI) policy template" on page 826.

See "Caldicott Report policy template" on page 802.

# Configuring keyword matching

Table 23-6 describes the components for implementing keyword matching.

**Table 23-6** Implementing keyword matching

Keyword matching feature	Description
Match on whole or partial keywords	Separate each keyword or phrase by a newline or comma.
and key phrases	See "Keyword matching examples" on page 587.
Match on the wildcard asterisk (*)	Match the wildcard at the end of a keyword, in whole word mode only.
character	See "Keyword matching examples" on page 587.
Keyword proximity matching	Match across a range of keywords.
	See "About keyword proximity" on page 586.
Find keywords	Implement one or more keywords in data identifiers to refine the scope of detection.
	See "Introducing data identifiers" on page 541.
Policy rules and exceptions	You can implement keyword matching conditions in policy rules and exceptions.
	See "Configuring the Content Matches Keyword condition" on page 591.
Cross-component matching	Keyword matching detects on one or more message components.
	See "Detection messages and message components" on page 305.
Keyword dictionary	If you have a large dictionary of keywords, you can index the keyword list.
	See "Use VML to generate and maintain large keyword dictionaries" on page 597.
CJK token verification	Enable on the detection server for CJK languages and match on whole words only.
	See Table 23-2 on page 585.

#### Configuring the Content Matches Keyword condition

The Content Matches Keyword condition lets you match content using keywords and key phrases.

See "Introducing keyword matching" on page 584.

You can implement keyword matching conditions in policy rules and exceptions.

See "Configuring policies" on page 326.

#### To configure the Content Matches Keyword condition

Add a new keyword condition to a policy rule or exception, or modify an existing one.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

2 Configure the keyword matching parameters.

See Table 23-7 on page 591.

See "Keyword matching syntax" on page 586.

Save the policy. 3

Table 23-7 Configure the Content Matches Keyword condition

Action	Description
Enter the match type.	Select if you want the keyword match to be:
	Case Sensitive or Case Insensitive
	Case insensitive is the default.
Choose the keyword	Select the keyword separator you to delimit multiple keywords:
separator.	Newline or Comma.
	Newline is the default.
Match any keyword.	Enter the keyword(s) or key phrase(s) you want to match. Use the separator you have selected (newline or comma) to delimit multiple keyword or key phrase entries.
	You can use the asterisk (*) wildcard character at the end of any keyword to match one or more suffix characters in that keyword. If you use the asterisk wildcard character, you must match on whole words only. For example, a keyword entry of <b>confid*</b> would match on "confidential" and "confide," but not "confine." As long as the keyword prefix matches, the detection engine matches on the remaining characters using the wildcard.
	See "Keyword matching syntax" on page 586.
	See "Keyword matching examples" on page 587.

Configure the Content Matches Keyword condition (continued) **Table 23-7** 

Action	Description
Configure keyword proximity matching (optional).	Keyword proximity matching lets you specify a range of detection among keyword pairs.
	See "About keyword proximity" on page 586.
(optional).	To implement keyword proximity matching:
	<ul> <li>Select (check) the Keyword Proximity matching option in the "Conditions" section of the rule builder interface.</li> <li>Click Add Pair of Keywords.</li> <li>Enter a pair of keywords.</li> <li>Specify the Word distance.</li> <li>The maximum distance between keywords is 999, as limited by the three-digit length of the</li> </ul>
	<ul> <li>"Word distance" field. The word distance is exclusive of detected keywords. For example, a word distance of 10 allows for a range of 12 words, including the two words comprising the keyword pair.</li> <li>Repeat the process to add additional keyword pairs.</li> </ul>
	The system connects multiple keyword pair entries the OR Boolean operator, meaning that the detection engine evaluates each keyword pair independently.
Match on whole or partial keywords.	Select the option <b>On whole words only</b> to match on whole keywords only (by default this option is selected).
	You must match on whole words only if you use the asterisk (*) wildcard character in any keyword you enter in the list.
	See "Keyword matching examples" on page 587.
	You must match on whole words only if you have enabled token validation for the server.
	See "Keyword matching examples for CJK languages" on page 588.
Configure match	Keyword matching lets you specify how you want to count condition matches.
conditions.	Select one of the following options:
	<ul> <li>Check for existence         The system reports one incident for all matches.     </li> <li>Count all matches and only report incidents with at least 1 matches (default)         With the default setting the system reports one incident for each match. Alternatively, you can configure the match threshold by changing the default value from 1 to another value.     </li> <li>See "Configuring match counting" on page 334.</li> </ul>

Table 23-7 Configur	e the Content Matches K	eyword condition	(continued)
---------------------	-------------------------	------------------	-------------

Action	Description
Select components	Keyword matching detection supports matching across message components.
to match on.	See "Selecting components to match on" on page 336.
	Select one or more message components to match on:
	<ul> <li>Envelope – Header metadata used to transport the message</li> <li>Subject – Email subject of the message (only applies to SMTP)</li> <li>Body – The content of the message</li> <li>Attachments – Any files attached to or transferred by the message</li> </ul>
	Note: On the endpoint the DLP Agent matches on the entire message, not individual components.  See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must be met to report a match.  You can <b>Add</b> any available condition from the list.  See "Configuring compound match conditions" on page 342.

#### Enabling and using CJK token verification for server keyword matching

To use token verification for Chinese, Japanese, and Korean (CJK) languages you must enable it on the server and you must use whole word matching for the keyword condition. In addition, there must be a sufficient amount of message text for the system to recognize the language.

See "Keyword matching examples for CJK languages" on page 588.

Table 23-8 lists and describes the detection server parameter that lets you enable token verification for CJK languages.

Keyword token verification parameter **Table 23-8** 

Setting	Default	Description
Keyword.TokenVerifierEnabled	false	Default is disabled ("false").  If enabled ("true"), the server validates tokens for Chinese, Japanese, and Korean language keywords.

Enable keyword token verification for CJK describes how to enable and use token verification for CJK keywords.

#### Enable keyword token verification for CJK

- 1 Log on to the Enforce Server as an administrative user.
- 2 Navigate to the System > Servers > Overview > Server Detail - Advanced Server Settings screen for the detection server you want to configure.
  - See "Advanced server settings" on page 203.
- 3 Locate the parameter **Keyword.TokenVerifierEnabled**.
- Change the value to **true** from **false** (default).
  - Setting the server parameter Keyword. TokenVerifierEnabled = true enables token validation for CJK keyword detection.
- Save the detection server configuration. 5
- 6 Recycle the detection server.
- Configure a keyword condition using whole word matching.
  - In the condition the option Match On whole word only is checked.
  - See "Configuring the Content Matches Keyword condition" on page 591.

#### Updating the Drug, Disease, and Treatment keyword lists for your HIPAA and Caldicott policies

If you have created a policy derived from the HIPAA or Caldicott template and have not made any changes or customizations to the derived policy, after upgrade you can create a new policy from the appropriate template and remove the old policy from production. If you have made changes to a policy derived from either the HIPAA or Caldicott policy template and you want to preserve these changes, you can copy the updated keyword lists from either the HIPAA or Caldicott policy template and use the copied keyword lists to update your HIPAA or Caldicott policies.

See "About updates to the Drug, Disease, and Treatment keyword lists" on page 589.

See "Keep the keyword lists for your HIPAA and Caldicott policies up to date" on page 596.

To update the Drug, Disease, and Treatment keyword lists for HIPAA and Caldicott policies provides instructions for updating the keyword lists for your HIPAA and Caldicot policies.

#### To update the Drug, Disease, and Treatment keyword lists for HIPAA and Caldicott policies

Create a new policy from a template and choose either the HIPAA or Caldicott template.

See "Creating a policy from a template" on page 312.

2 Edit the detection rules for the policy.

See "Configuring policy rules" on page 330.

- Select the Patient Data and Drug Keywords (Keyword Match) rule. 3
- 4 Select the Content Matches Keyword condition.
- Select all the keywords in the **Match any Keyword** data field and copy them to the Clipboard.
- 6 Paste the copied keywords to a text file named Drug Keywords.txt.
- 7 Cancel the rule edit operation to return to the policy **Detection** tab.
- 8 Repeat the same process for the Patient Data and Treatment Keywords (Keyword Match) rule.
- 9 Copy and paste the keywords from the condition to a text file named Treatment Keywords.txt.
- 10 Repeat the same process for the Patient Data and Disease Keywords (Keyword Match) rule.
- 11 Copy and paste the keywords from the condition to a text file named Disease Keywords.txt.
- 12 Update your HIPAA and Caldicott policies derived from the HIPAA or Caldicott templates using the keyword \*.txt files you created.
- 13 Test your updated HIPAA and Caldicott policies.

# Best practices for using keyword matching

The Content Matches Keyword condition lets you match content using keywords, key phrases, and keyword lists or dictionaries. On the server, the keyword rule matches on the header, subject, body and attachment message components, and it supports cross-component matching. On the endpoint the keyword condition matches on the entire message.

Table 23-9 summarizes the keyword matching best practices in this section.

Best practice	More information
Enable linguistic validation for CJK keyword detection on the server.	See "Enable token verification on the server to reduce false positives for CJK keyword detection" on page 596.
Update keyword lists for your Caldicott and HIPAA policies.	See "Keep the keyword lists for your HIPAA and Caldicott policies up to date" on page 596.
Tune keyword validators to improve data identifier accuracy.	See "Tune keywords lists for data identifiers to improve match accuracy" on page 597.
Use VML to profile long keyword lists and dictionaries	See "Use VML to generate and maintain large keyword dictionaries" on page 597.
Use keyword matching for metadata detection.	See "Use keyword matching to detect document metadata" on page 597.

Summary of keyword matching best practices **Table 23-9** 

#### Enable token verification on the server to reduce false positives for CJK keyword detection

Symantec Data Loss Prevention provides token validation for Chinese, Japanese, and Korean (CJK) languages. Token validation is supported for detection servers and must be enabled.

See "About keyword matching for Chinese, Japanese, and Korean (CJK) languages" on page 585.

Token validation lets you match CJK keywords using whole word matching, and improves overall match accuracy for CJK languages. Although there may be a slight performance hit, you should enable token verification for each detection server where CJK keyword conditions are deployed. Once enabled you can use whole word matching for CJK keywords.

See "Enabling and using CJK token verification for server keyword matching" on page 593.

#### Keep the keyword lists for your HIPAA and Caldicott policies up to date

For each Symantec Data Loss Prevention relese, the Drug, Disease, and Treatment keyword lists are updated based on information from the U.S. Federal Drug Administration (FDA) and other sources. These keyword lists are used in the HIPAA and HITECH (including PHI) and Caldicott Report policy templates.

See "About updates to the Drug, Disease, and Treatment keyword lists" on page 589.

If you have upgraded to the latest Data Loss Prevention version and you have existing policies derived from either the HIPAA or Caldicott policy template, consider updating your HIPAA and Caldicott policies to use the Drug, Disease, and Treatment keyword lists provided with this Data Loss Prevention version.

See "Updating the Drug, Disease, and Treatment keyword lists for your HIPAA and Caldicott policies" on page 594.

#### Tune keywords lists for data identifiers to improve match accuracy

Many data identifier definitions contain required keyword validators with prepopulated keyword lists. In addition, you can add your own list of keywords to a data identifier rule. The best practice is tune the keyword list using a keyword matching condition before you add the keyword list to the data identifier condition as a required or optional validator

See "Using pattern validators" on page 575.

To tune the keyword list, take the keywords you want to use for the validator and put them into a separate keyword matching rule condition and policy. Then test the policy using data that should and should not match the keywords. The keyword rule will let you see match highlighting and tune the keyword list. Once tested, you can add the keywords to the data identifier and then test the data identifier policy to ensure accuracy.

#### Use keyword matching to detect document metadata

Symantec Data Loss Prevention supports metadata detection for certain document formats, such as DOCX and PDF. Detection servers and DLP Agents support metadata detection.

If you want to detect document metadata, the recommendation is to enable it for the server or endpoint and use the Content Matches Keyword condition to match metadata tags.

#### Use VML to generate and maintain large keyword dictionaries

Sometimes you may want to protect a long list or dictionary of keywords. An example might be a list of project code names. You can use Vector Machine Learning (VML) to automate the detection of long keyword lists that are difficult to generate, tune, and maintain. For example, you could generate a VML profile based on a collection of documents containing the keywords you want to detect. If you want to detect common words, remove them from the VML stopword file.

See "Best practices for using VML" on page 532.

# Detecting content using regular expressions

This chapter includes the following topics:

- Introducing regular expression matching
- About writing regular expressions
- Configuring the Content Matches Regular Expression condition
- Best practices for using regular expression matching

# Introducing regular expression matching

Data Loss Prevention provides the **Content Matches Regular Expression** policy match condition to match message content using the regular expression pattern language.

Regular expressions provide a mechanism for identifying strings of text, such as particular characters, words, or patterns of characters. You can use the regular expression condition is used to match (or exclude from matching) characters, patterns, and strings.

See "Configuring the Content Matches Regular Expression condition" on page 600.

See "Best practices for using regular expression matching" on page 601.

# About writing regular expressions

Symantec Data Loss Prevention implements the Java regular expression syntax for policy condition matching. provides some reference constructs for writing regular expressions to match or exclude characters in messages or message components.

See "Introducing regular expression matching" on page 598.

Note: Data Identifier pattern matching is based on the regular expression syntax. However, not all regular expression constructs listed in the table below are supported by Data Identifier patterns. See "About data identifier patterns" on page 547.

**Table 24-1** Regular expression constructs

Regular expression construct	Description
	Any single character (except for newline characters)
	<b>Note:</b> The use of the dot ( . ) character is not supported for data identifier patterns.
\d	Any digit (0-9)
\s	Any white space
\w	Any word character (a-z, A-z, 0-9, _)
	<b>Note:</b> The use of the $\setminus_{\mathbb{W}}$ construct does not match the underscore (_) character when implemented in a data identifier pattern.
\D	Anything other than a digit
\S	Anything other than white space
[]	Elements inside brackets are a character class (For example, [abc] matches 1 character: a, b, or c.)
^	At the beginning of a character class, negates it (For example, [^abc] matches anything except a, b, or c.)
+	Following a regular expression means 1 or more (For example, \d+ means 1 or more digit.)
?	Following a regular expression means 0 or 1 (For example, \d? means 1 or no digits.)
*	Following a regular expression means any number (For example, \d* means 0, 1, or more digits.)
(?i)	At the beginning of a regular expression makes it case-insensitive (Regular expressions are case-sensitive by default.)
(?: )	Groups regular expressions together (The ?: is a slight performance enhancement.)
(?u)	Makes a period (.) match even newline characters
T	Means OR (For example, A   B means regular expression A or regular expression B.)

# **Configuring the Content Matches Regular Expression** condition

You use the Content Matches Regular Expression condition to match (or exclude from matching) characters, patterns, and strings using regular expressions.

See "Introducing regular expression matching" on page 598.

To configure the Content Matches Regular Expression condition

Add a Content Matches Regular Expression condition to a policy, or edit an existing one.

See "Configuring policies" on page 326.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

Configure the **Content Matches Regular Expression** condition parameters. See Table 24-2 on page 600.

3 Save the policy configuration.

**Table 24-2** Content Matches Regular Expression parameters

Action	Description
Match regex.	Specify a regular expression to be matched.
	See "About writing regular expressions" on page 598.
Configure match	Configure how you want to count matches.
counting. See "Configuring match counting" on page 334.	See "Configuring match counting" on page 334.
	Check for existence reports a match count of 1 if there are one or more matches. For compound rules or exceptions, all conditions must be configured this way.
	<b>Count all matches</b> reports the sum of all matches; applies if any condition uses this parameter.

Table 24-2 Content Matches Regular Expression parameters (continued)

Action	Description	
Match on one or more message components.	company to the compan	
	<ul> <li>Envelope – The header of the message, transport metadata.</li> <li>Subject – The email subject (only applies to email messages).</li> <li>Body – The content of the message.</li> <li>Attachments – The content of any files that are attached to or transported by the message.</li> </ul>	
	See "Selecting components to match on" on page 336.  Note: On the endpoint the DLP Agent matches the entire message regardless of any individually selected components. See "Detection messages and message components" on page 305.	
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.  You can <b>Add</b> any available condition from the list.  See "Configuring compound match conditions" on page 342.	

# Best practices for using regular expression matching

This section provides considerations for implementing the Content Matches Regular **Expression** match condition in your Data Loss Prevention policies.

See "Introducing regular expression matching" on page 598.

Table 24-3 summarizes the regular expression matching best practices in this section.

Table 24-3 Regular Expressions best practices

Best practice	Description
Use Data Identifiers instead of regular expressions where possible.	See "Use regular expressions sparingly to support efficient performance" on page 603.
Use regular expressions sparingly to support efficent policy performance.	See "Test regular expressions before deployment to improve accuracy" on page 603.
Use look ahead and behind characters to improve regex performance.	See "Use look ahead and look behind characters to improve regex accuracy" on page 602.

**Table 24-3** Regular Expressions best practices (continued)

Best practice	Description
Test regular expressions for accuracy and performance.	See "Use look ahead and look behind characters to improve regex accuracy" on page 602.

#### When to use regular expression matching

Data Identifiers are more efficient than regular expressions because the Data Identifier patterns are tuned for accuracy and the data is validated. For example, if you want to search for social security numbers, use the US Social Security Number (SSN) Data Identifier instead of a regular expression.

The regular expression condition is useful for matching or excepting unique data types for which there are no system-provided Data Identifiers. Examples of these might include internal account numbers and data types that can vary greatly in length, such as email addresses.

#### Use look ahead and look behind characters to improve regex accuracy

Symantec Data Loss Prevention implements a significant enhancement to improve the performance of regular expressions. To achieve improved regex performance, the look ahead and look behind sections must exactly match one of the supported standard sections.

Table 24-4 lists the standard look ahead and look behinds sections that this performance improvement supports. If either section differs even slightly, that section is executed as part of the regular expression without the performance improvement.

See "About writing regular expressions" on page 598.

Look ahead and look behind standard sections **Table 24-4** 

Operation	Construct
Look ahead	(?=(?:[^-\w]) \$)
Look behind	(?<=(^ (?:[^)+\d][^-\w+])))
	and
	(?<=(^ (?:[^)+\d][^-\w+]) \t))

#### Use regular expressions sparingly to support efficient performance

Regular expressions can be computationally expensive. If you add a regular expression condition, observe the system for one hour. Make sure that the system does not slow down and that there are no false positives.

#### Test regular expressions before deployment to improve accuracy

If you implement regular expression matching, consider using a third-party tool to test the regular expressions before you deployment the policy rules to production. The recommended tool is RegexBuddy. Another good tool for texting your regular expressions is RegExr.

# Detecting international language content

This chapter includes the following topics:

- Detecting non-English language content
- Best practices for detecting non-English language content

# **Detecting non-English language content**

Symantec Data Loss Prevention detection features support many localized versions of Microsoft Windows operating systems. To use international character sets, the Windows system on which you view the Enforce Server administration console must have the appropriate capabilities.

See "About support for character sets, languages, and locales" on page 64.

See "Working with international characters" on page 67.

You can create policies and detect violations using any supported language. You can use localized keywords, regular expressions, and Data Profiles to detect data loss. In addition, Symantec Data Loss Prevention offers several international data identifiers and policy templates for protecting confidential data.

See "Supported languages for detection" on page 65.

See "Use international policy templates for policy creation" on page 605.

See "Use custom keywords for system data identifiers" on page 606.

### Best practices for detecting non-English language content

This section provides some best practices for implementing non-English language conent detection.

#### Upgrade to the latest version of Data Loss Prevention

Symantec Data Loss Prevention version 12.5 includes several enhancements for Asian language detection, including multi-token EDM and linguistic validation for Chinese, Japanese, and Korean (CJK) keywords. To take advantage of these enhancements, upgrade your servers to the latest version and update your Exact Data profiles.

See "Updating EDM indexes to version 12.5" on page 416.

See "Enable token validation to match Chinese, Japanese, and Korean keywords on the server" on page 608.

#### Use international policy templates for policy creation

Symantec Data Loss Prevention provides several international policy templates that you can quickly deploy in your enterprise.

See "Creating a policy from a template" on page 312.

Table 25-1 International policy templates

Policy template	Description
Canadian Social Insurance Numbers	This policy detects patterns indicating Canadian social insurance numbers.
	See "Canadian Social Insurance Numbers policy template" on page 804.
Caldicott Report	This policy protects UK patient information.
	See "Caldicott Report policy template" on page 802.
UK Data Protection Act 1998	This policy protects personal identifiable information.
	See "Data Protection Act 1998 (UK) policy template" on page 810.
EU Data Protection Directives	This policy detects personal data specific to the EU directives.
	See "Data Protection Directives (EU) policy template" on page 811.
UK Human Rights Act 1998	This policy enforces Article 8 of the act for UK citizens.
	See "Human Rights Act 1998 policy template" on page 830.

Policy template	Description
PIPEDA (Canada)	This policy detects Canadian citizen customer data.
,	See "PIPEDA policy template" on page 846.
SWIFT Codes (International banking)	This policy detects codes that banks use to transfer money across international borders.
	See "SWIFT Codes policy template" on page 862.
UK Drivers License Numbers	This policy detects UK Drivers License Numbers.
	See "UK Drivers License Numbers policy template" on page 863.
UK Electoral Roll Numbers	This policy detects UK Electoral Roll Numbers.
	See "UK Electoral Roll Numbers policy template" on page 864.
UK National Insurance Numbers	This policy detects UK National Insurance Numbers.
	See "UK National Insurance Numbers policy template" on page 864.
UK National Health Service Number	This policy detects personal identification numbers issued by the NHS.
	See "UK National Health Service (NHS) Number policy template" on page 864.
UK Passport Numbers	This policy detects valid UK passports.
	See "UK Passport Numbers policy template" on page 865.
UK Tax ID Numbers	This policy detects UK Tax ID Numbers.
	See "UK Tax ID Numbers policy template" on page 865.

**Table 25-1** International policy templates (continued)

#### Use custom keywords for system data identifiers

Data identifiers offer broad support for detecting international content.

See "Introducing data identifiers" on page 541.

Some international data identifiers offer a wide breadth of detection only. In this case you can implement the Find Keywords optional validator to narrow the scope of detection. Implementing this optional validator may help you eliminate any false positives that your policy matches.

See "Selecting a data identifier breadth" on page 555.

The following table provides keywords for several international data identifiers.

#### To use international keywords for system data identifiers

1 Create a policy using one of the system-provided international data identifiers that is listed in the table.

Table 25-2

2 Select the **Find Keywords** optional validator.

See "Configuring the Content Matches data identifier condition" on page 552.

3 Copy and past the appropriate comma-separated keywords from the list to the Find Keywords optional validator field.

See "Configuring optional validators" on page 559.

Table 25-2 International data identifiers and keyword lists

			-
Data Identifier	Language	Keywords	English Translation
Burgerservicenummer (BSN)	Dutch	Persoonsnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden	person number, social-fiscal number (abbreviation), social-fiscal number, person-related number
Codice Fiscale	Italian	codice fiscal, dati anagrafici, partita I.V.A., p. iva	tax code, personal data, VAT number, VAT number
French INSEE Code	French	INSEE, numéro de sécu, code sécu	INSEE, social security number, social security code
Hong Kong ID	Chinese (Traditional)	身份證,三顆星	Identity card, Hong Kong permanent resident ID Card
International Bank Account Number (IBAN) Central	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
International Bank Account Number (IBAN) East	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
International Bank Account Number (IBAN) West	French	Code IBAN, numéro IBAN	IBAN Code, IBAN number
People's Republic of China ID	Chinese (Simplified)	身份证,居民信息,居民身份信息	Identity Card, Information of resident, Information of resident identification
South Korea Resident Registration Number	Korean	주민등록번호, 주민번호	Resident Registration Number, Resident Number

Data Identifier	Language	Keywords	English Translation
Spanish DNI ID	Spanish	DNI	DNI
Swiss AHV Number	French	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité soclale, Numéro AVH	AVS number, insurance number, national identifier, national insurance number, social security number, AVH number
	German	AHV-Nummer, Matrikelnumme, Personenidentifikationsnummer	AHV number, Swiss Registration number, PIN
	Italian	AVS, AVH	AVS, AVH
Taiwan ID	Chinese (Traditional)	中華民國國民身分證	Taiwan ID

Table 25-2 International data identifiers and keyword lists (continued)

#### Enable token validation to match Chinese, Japanese, and Korean keywords on the server

The Content Matches Keyword condition supports both whole word and partial word matching.

Symantec Data Loss Prevention detection servers support natural language processing for Chinese, Japanese, and Korean (CJK) language keywords. If you want to detect CJK keywords, the recommendation is to enable token validation on the detection server and to use whole word matching for the keyword condition.

The DLP Agent does not support token validation for CJK. On the endpoint, for CJK and mixed-language keyword matching, consider using partial word matching.

With whole word matching, keywords match at word boundaries only (\W in the regular expression lexicon). Any characters other than A-Z, a-z, and 0-9 are interpreted as word boundaries. With whole word matching, keywords must have at least one alphanumeric character (a letter or a number). A keyword consisting of only white-space characters, such as "..", is ignored.

See "About keyword matching for Chinese, Japanese, and Korean (CJK) languages" on page 585.

# Detecting file properties

This chapter includes the following topics:

- Introducing file property detection
- Configuring file property matching
- Best practices for using file property matching

# Introducing file property detection

Symantec Data Loss Prevention provides various methods for detecting the context of messages, files, and attachments. You can detect the type, size, and name of files and attachments. You can also use these conditions to except files and attachments from matching.

See "About file type matching" on page 609.

See "About file size matching" on page 611.

See "About file name matching" on page 611.

See "Configuring file property matching" on page 611.

#### About file type matching

You use the **Message Attachment or File Type Match** condition to match the file type of a message attachment. Symantec Data Loss Prevention supports the identification of over 300 file types.

See "Supported formats for file type identification" on page 669.

Example uses of message attachment and file type matching are as follows:

 A certain type of document should never leave the organization (such as a PGP document or EXE file).  A certain type of match is likely to occur only in a document of a certain type, such as a Word document.

The detection engine does not rely on the file name extension to match file format type. For example, if a user changes the .mp3 file name extension to .doc and emails the file, the detection engine can still register a match because it checks the binary signature of the file to detect it as an MP3 file.

Note: File type matching does not crack the file and detect content; it only detects the file type based on the binary signature of the file. To detect content, use a content matching condition.

See "Configuring the Message Attachment or File Type Match condition" on page 612.

See "About custom file type identification" on page 610.

#### About file format support for file type matching

Symantec Data Loss Prevention supports over 300 file formats for file type identification using the Message Attachment or File Type Match policy condition.

Refer to the following link for a complete list of file formats that can be recognized by this policy condition.

See "Supported formats for file type identification" on page 669.

#### About custom file type identification

If the type of file you want to detect is not supported as a system default file type, Symantec Data Loss Prevention provides you with the ability to identify custom file types using scripts.

To detect a custom file type, you use the Symantec Data Loss Prevention Scripting Language to write a custom script that detects the binary signature of the file format that you want to protect. To implement this match condition you need to enable it on the Enforce Server.

See "Enabling the Custom File Type Signature condition in the policy console" on page 616.

See "Configuring the Custom File Type Signature condition" on page 617.

Refer to the Symantec Data Loss Prevention Detection Customization Guide for the language syntax and examples.

Note: The Symantec Data Loss Prevention Scripting Language only identifies custom file formats; it does not extract content from custom file types.

#### About file size matching

You use the Message Attachment or File Size Match condition to detect the size of the message body and attachment. Detection is based on either the body or attachment message component, or both, but not the entire message.

For example, consider a condition where you specify that an attachment size greater than 50k matches. A message with a 5k header, 10k body, and 55k attachment matches because the detected message component is the attachment, which in this case is over the 50k threshold. On the other hand, a message with a 5k header, 10k body, and 45k attachment does not match, even though the entire message is more than 50k.

See "Detection messages and message components" on page 305.

See "Configuring the Message Attachment or File Size Match condition" on page 613.

#### About file name matching

You use the Message Attachment or File Name Match condition to detect the names of files and attachments.

See "File name matching syntax" on page 615.

See "File name matching examples" on page 615.

See "Configuring the Message Attachment or File Name Match condition" on page 614.

# Configuring file property matching

Table 26-1 lists the conditions available for implementing file property matching.

**Table 26-1** File Properties match conditions

Match condition	Description
Message Attachment or File Type Match	Detect or except specific files and attachments by type.  See "About file type matching" on page 609.
	See "Configuring the Message Attachment or File Type Match condition" on page 612.

Match condition	Description	
Message Attachment or File Size Match	Detect or except specific files and attachments by size.	
	See "About file size matching" on page 611.	
	See "Configuring the Message Attachment or File Size Match condition" on page 613.	
Message Attachment or File Name Match	Detect or except specific files and attachments by name.	
	See "About file name matching" on page 611.	
	See "Configuring the Message Attachment or File Name Match condition" on page 614.	
Custom File Type Signature	Detect or except custom file types.	
Message/Email Properties and Attributes	Detect email properties for Data Classification services.	
	See "Configuring the Classify Enterprise Vault Content response action" on page 915.	
	See the Enterprise Vault Data Classification Services Implementation Guide.	

**Table 26-1** File Properties match conditions (continued)

#### Configuring the Message Attachment or File Type Match condition

The Message Attachment or File Type Match condition matches the file type of an attachment message component. You can configure an instance of this condition in policy rules and exceptions.

See "About file type matching" on page 609.

#### To configure the Message Attachment or File Type Match condition

Add a Message Attachment or File Type Match condition to a policy rule or exception, or edit an existing one.

See "Configuring policies" on page 326.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

Configure the **Message Attachment or File Type Match** condition parameters.

See Table 26-2 on page 613.

3 Click Save to save the policy.

**Table 26-2** Message Attachment or File Type Match condition parameters

Action	Description					
Select the file type or types	Select all of the formats you want to match.					
to match.	See "Supported formats for file type identification" on page 669.					
	Click select all or deselect all to select or deselect all formats.					
	To select all formats within a certain category (for example, all word-processing formats), click the section heading.					
	The system implies an OR operator among all file types you select. For example, if you select Microsoft Word and Microsoft Excel file type attachments, the system detects all messages with Word or Excel documents attached, not messages with both attachment types					
Match on attachments only.	This condition only matches on the <b>Message Attachments</b> component.					
	See "Detection messages and message components" on page 305.					
Also match on one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.					
	You can <b>Add</b> any condition available from the list.					
	See "Configuring compound match conditions" on page 342.					

#### Configuring the Message Attachment or File Size Match condition

The Message Attachment or File Size Match condition matches or excludes from matching files of a specified size. You can configure an instance of this condition in policy rules and exceptions.

See "About file size matching" on page 611.

#### To configure the Message Attachment or File Size Match condition

Add a Message Attachment or File Size Match condition to a policy, or edit an existing one.

See "Configuring policies" on page 326.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

Configure the **Message Attachment or File Type Match** condition parameters.

See Table 26-3 on page 614.

3 Click Save to save the policy.

	-
Action	Description
Enter the Size to match.	Enter a number, and select the unit of measure: <b>bytes</b> , kilobytes ( <b>KB</b> ), megabytes ( <b>MB</b> ), or gigabytes ( <b>GB</b> ).
	Select More Than to specify the minimum size of the file to match.
	Select Less Than to specify the maximum size of the file to match.
Match on the body or	Select one or both of the following message components on which to base the match:
attachments.	■ Body – The content of the message.
	■ Attachments – Any files that are attached to or transferred by the message.
	See "Selecting components to match on" on page 336.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

**Table 26-3** Message Attachment or File Size Match parameters

#### Configuring the Message Attachment or File Name Match condition

The Message Attachment or File Name Match condition matches based on the name of a file attached to the message. You can configure an instance of this condition in policy rules and exceptions.

See "About file name matching" on page 611.

#### To configure the Message Attachment or File Name Match condition

Add a Message Attachment or File Name Match condition to a policy, or edit an existing one.

See "Configuring policies" on page 326.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

2 Configure the Message Attachment or File Type Match condition parameters.

See Table 26-4 on page 615.

3 Click **Save** to save the policy.

Action	Description
Specify the File Name.	Specify the file name to match using the DOS pattern matching language to represent patterns in the file name.
	Separate multiple matching patterns with commas or by placing them on separate lines.
	See "File name matching syntax" on page 615.
	See "File name matching examples" on page 615.
Match on attachments.	This condition only matches on the Message Attachments component.
	See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

**Table 26-4** Message Attachment or File Name Match parameters

#### File name matching syntax

For file name matching, the system supports the DOS pattern matching syntax to detect file names, including wildcards.

See "About file name matching" on page 611.

Any characters you enter (other than the DOS operators) match exactly. To enter multiple file names, enter them as comma-separated values or by line space.

Table 26-5 describes the syntax for the Message Attachment or File Name Match condition.

Table 26-5	υ	U	15	(	Į	96	er	a	tc	rs	10	r t	П	е	name	; d	etec	tior	1
------------	---	---	----	---	---	----	----	---	----	----	----	-----	---	---	------	-----	------	------	---

Operator	Description
	Use a dot to separate the file name and the extension.
*	Use an asterisk as a wild card to match any number of characters (including none).
?	Use a question mark to match a single character.

#### File name matching examples

Table 26-6 lists some examples for matching file names using the **Message** Attachment or File Name condition.

See "About file name matching" on page 611.

**Table 26-6** File name matching examples

Match objective	Example
To match a Word file name that begins with ENG- followed by any eight characters:	ENG-???????.doc
If you are not sure that it is a Word document:	ENG-???????.*
If you are not sure how many characters are in the name:	ENG-*.*
To match all file names that begin with ENG- and all file names that begin with ITA-:	Enter as comma separated values:  ENG-*.*,ITA-*
	Or separate the file names by line space:
	ENG-*.*
	ITA-*

#### Enabling the Custom File Type Signature condition in the policy console

By default the **Custom File Type Signature** policy condition is not enabled. To implement the Custom File Type Signature condition, you must first enable it.

See "About custom file type identification" on page 610.

#### To enable the Custom File Type Signature rule

- 1 Using a text editor, open the file \SymantecDLP\Protect\config\Manager.properties
- 2 Set the value of the following parameter to "true":

```
com.vontu.manager.policy.showcustomscriptrule=true
```

- 3 Stop and then restart the Vontu Manager service.
- Log back on to the Enforce Server Administration Console and add a new blank policy.
- Add a new detection rule or exception and beneath the File Properties heading you should see the Custom File Type Signature condition.
- Configure the condition with your custom script. See "Configuring the Custom File Type Signature condition" on page 617.

#### Configuring the Custom File Type Signature condition

The Custom File Type Signature condition matches custom file types that you have scripted. You can implement the Custom File Type Signature condition in policy rules and exceptions.

See "About custom file type identification" on page 610.

See "Enabling the Custom File Type Signature condition in the policy console" on page 616.

#### To configure a Custom File Type Signature condition

Add a Custom File Type Signature condition to a policy rule or exception, or edit an existing one.

See "Configuring policy rules" on page 330.

See "Configuring policy exceptions" on page 340.

2 Configure the Custom File Type Signature condition parameters.

See Table 26-7 on page 617.

3 Click Save to save the policy.

**Table 26-7** Custom File Type Signature parameters

Action	Description	
Enter the Script Name.	Specify the name of the script. The name must be unique across policies.	
Enter the custom file type script.	Enter the File Type Matches Signature script for detecting the binary signature of the cu file type.	
	See the Symantec Data Loss Prevention Detection Customization Guide for details on writing custom scripts.	
Match only on	This condition only matches on the Message Attachments component.	
attachments.	See "Detection messages and message components" on page 305.	
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.	
	You can <b>Add</b> any condition available from the list.	
	See "Configuring compound match conditions" on page 342.	

#### Best practices for using file property matching

This section provides best practices for using file property matching conditions to match file formats, file size, and file name.

#### Use compound file property rules to protect design and multimedia files

You can use IDM to protect files, or you can use file property rules. Unless you must protect an exact file, the general recommendation is to use the file property rules because there is less overhead in setting up the rules.

For example, if you want to detect CAD files that contain IP diagrams, you could index these files and apply IDM rules to detect them. Alternatively, you could create a policy that contains a file type rule that detects on the CAD file format plus a file size rule that specifies a threshold size. The file property approach is preferred because in this scenario all you really care about is protecting large CAD files potentially leaving the company. There is no need to gather and index these files for IDM if you can simply create rules that will detect on the file type and the size.

#### Do not use file type matching to detect content

File type recognition does not crack the file and detect content; it only detects the file type based on the file's binary signature. To detect content, use a content detection rule such as EDM, IDM, Data Identifiers, or Keyword matching.

For custom file type detection, use the DLP Scripting Language. Refer to the Symantec Data Loss Prevention Detection Customization Guide.

#### Calculate file size properly to improve match accuracy

The file size method counts both the body and any attachments in the file size you specify.

#### Use expression patterns to match file names

The following DOS pattern matching expressions are provided as examples for configuring the Message Attachment or File Name condition.

**Table 26-8** File name detection examples

#### Example

Any characters you enter (other than the DOS operators) match exactly.

For example, to match a Word file name that begins with ENG- followed by any eight characters, enter: ENG-??????doc

If you are not sure that it is a Word document, enter: ENG-???????.\*

If you are not sure how many characters follow ENG-, enter: ENG-\*.\*

To match all file names that begin with ENG- and all file names that begin with ITA-, enter: ENG-\*.\*,ITA-\* (comma separated), or you can separate the file names by line space.

#### Use scripts and plugins to detect custom file types

Symantec Data Loss Prevention provides two mechanisms for detecting custom file types: the DLP Scripting Language and the Content Extraction SPI. If the only requirement is file type recognition, it may be easier to write a script than an SPI plugin. But, there may be occasions where using a script is inadequate.

The scripting language does not support loops; you cannot iterate over the file type bytes and do some processing. The scripting language is designed to detect a known signature at a relatively known offset. You cannot use the scripting language detect subtypes of the same document type. For example, , if you wanted to detect password protected PDF files, you could not use the scripting language. Or, if you wanted to detect only Word documents with track changes enabled, you would have to write a plugin. On the other hand, you can deploy a script to the endpoint; currently plugins are server-based only.

For more information, refer to the Symantec Data Loss Prevention Content Extraction Plugin Developers Guide and the Symantec Data Loss Prevention Detection Customization Guide on writing custom plugins and scripts, respectively.

# Detecting email for data classification services

This chapter includes the following topics:

- About implementing detection for Enterprise Vault Classification
- About matching on the message Subject for Data Classification Services
- Enabling classification test mode
- Configuring the Message/Email Properties and Attributes condition

# About implementing detection for Enterprise Vault Classification

You can use the full policy authoring functionality of Symantec Data Loss Prevention, along with a new **Message/Email Properties and Attributes** detection rule, to automatically classify messages with Enterprise Vault for Microsoft Exchange. A new classification response rule produces a classification result that indicates whether a message should be archived or deleted. The Classification Server returns the classification result to the Enterprise Vault filter. Enterprise Vault can then use the result to perform archiving, delete messages, and flag messages for compliance reviews or E-Discovery searches.

**Note:** The Classification Server is used only with the Symantec Data Classification for Enterprise Vault solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Enterprise Vault Data Classification Services filter and Classification Server to communicate with one another. See the *Symantec Enterprise Vault Data Classification Services Implementation Guide* for more information.

The following table highlights the key policy configuration components that are associated with Data Classification for Enterprise Vault.

Table 27-1 Policy configuration for data classification

Configuration type	Торіс
Policy actions to enable classification test mode and limit generated classification results	See "Enabling classification test mode" on page 621.
Message/Email Properties and Attributes detection condition	See "Configuring the Message/Email Properties and Attributes condition" on page 623.
Classify Enterprise Vault Content response rule action	See "Configuring the Classify Enterprise Vault Content response action" on page 915.

#### About matching on the message Subject for Data Classification Services

Symantec Data Loss Prevention provides the ability to detect content in the Subject component of a message, independent of other components in the message envelope. You can use the Subject component to match on Exchange messages delivered from a Classification Server. The **Envelope** component is not applicable to Exchange email delivered from a Classification Server. See the Enterprise Vault Data Classification Services Implementation Guide for more information.

See "Detection messages and message components" on page 305.

See "Selecting components to match on" on page 336.

See "Configuring the Message/Email Properties and Attributes condition" on page 623.

#### **Enabling classification test mode**

When you create or configure any policy (Manage > Policies > Policy List), the Configure Policy screen contains options in the Policy Actions section that apply only to classification policies. You may choose to place Classification policies in test mode during the initial configuration of your Data Classification for Enterprise Vault deployment, or while tuning individual classification policies. When a classification policy runs in test mode, the Classification Server adds a test mode tag to any classification results that are returned to the Enterprise Vault Data Classification Filter for that policy. Enterprise Vault for Microsoft Exchange uses

the tag to ignore the outcome of the classification response for that policy, but still performs archiving as if no classification service is running

When a classification policy runs in test mode, the Enforce Server creates a classification event each time a message matches the policy. You can view these classification events in the incident lists of the Enforce Server administration console (Incidents > Classification). The test mode configuration also enables you to limit the number of classification events that are recorded.

Note: The Enforce Server creates classification events only for those policies that run in test mode. When you disable test mode for production use, no classification incidents are recorded for that policy.

After you are confident that the classification policy works as intended, you can disable test mode so that Enterprise Vault actively classifies or deletes messages as defined in the policy.

Note: The parameters that are listed have no effect unless the policy uses the Classification: Classify Enterprise Vault Content response rule.

Table 27-2 Classifying policy detection matches

Parameter	Description
Enable Classification Test Mode	This setting is enabled by default and adds a test mode flag to the policy detection result for this policy. The flag indicates that Enterprise Vault should perform no action for the returned classification result.  To classify Enterprise Vault content using this policy, uncheck
	this option.
Maximum for Classification Test Mode Events	This setting specifies the maximum number of classification events that Symantec Data Loss Prevention creates for this policy while in test mode. Limit the number of classification events for test mode policies, because each message that is posted to the Classification Server should generate a classification result. Specify a limit that enables you to evaluate the performance of your classification policy. You may choose to delete these classification events from the Enforce Server database after you activate the policy (disable test mode). The default setting records a maximum of 100 events.
	You can view recorded test-mode classification events by selecting <b>Incidents &gt; Classification</b> .

### Configuring the Message/Email Properties and Attributes condition

The Message/Email Properties and Attributes detection rule enables you to classify Microsoft Exchange email messages based on specific message attributes. This detection rule is only applied to Microsoft Exchange messages that are delivered from a Data Classification for Enterprise Vault filter to a Classification Server.

Note: The Classification Server is used only with the Symantec Data Classification for Enterprise Vault solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Data Classification for Enterprise Vault filter and Classification Server to communicate with one another. See the Symantec Enterprise Vault Data Classification Services Implementation Guide for more information.

The Message/Email Properties and Attributes detection rule examines the various Messaging Application Programming Interface (MAPI) properties and attributes that Exchange has assigned to the email. Use these attributes to determine whether a message should be archived or deleted, and whether to flag the message for compliance review or E-Discovery searches.

**Table 27-3** Message/Email Properties and Attributes condition parameters

MAPI Attribute	Description
Message Sensitivity	This attribute describes the sensitivity of the message.  Select Message Sensitivity and then select one or more of the following sensitivity levels:  Normal Personal Confidential  The detection rule matches if the message contains any of the selected Message Sensitivity levels.

# Message/Email Properties and Attributes condition parameters

**Table 27-3** 

Table 27-3	(continued)
MAPI Attribute	Description
Message Class	This attribute describes the type of message, or the type of content that the message contains. Select <b>Message Class</b> and then select one or more classes from the <b>Available Message Classes</b> column. Use the arrows to move selected classes into the <b>Selected Message Classes</b> column.
	The following classes of interpersonal messages (IPM) appear in the Available Message Classes column:
	<ul> <li>IPM.Activity*—Journal entries, business notes, and phone logs.</li> <li>IPM.Appointment*—Calendar appointments.</li> <li>IPM.Contact*—Accounts and business contacts.</li> <li>IPM.Document*—Document files.</li> </ul>
	<ul> <li>IPM.Note*—Email messages that were received from a MAPI source (Exchange email).</li> <li>IPM.Post*—Email messages that were received from an SMTP source, rather than a MAPI source.</li> <li>IPM.Stickynote*—Notes.</li> </ul>
	<ul> <li>IPM.Task*—Tasks, projects, and campaigns.</li> <li>REPORT.IPM.*—Message delivery and non-delivery receipts, message read receipts, and message disposition notifications.</li> </ul>
	Certain message classes, such as IPM.Note, can be classified both when journal and mailbox archiving is enabled in Enterprise Vault for Microsoft Exchange. Other classes, such as IPM.contact, IPM.task, and IPM.Appointment are not present in the journal and are classified only when Enterprise Vault performs mailbox archiving.
	Use the <b>Other</b> field to specify message classes to examine in addition to or in place of those classes that are listed in the <b>Available Message Classes</b> column. Use the asterisk wildcard to specify multiple message subclasses. Ensure that any new mailbox classes that you add are also specified in the <b>Exchange Message Classes and Exchange Mailbox Policy &gt; Message Classes</b> tab in Enterprise Vault. (Enterprise Vault archives all journal classes that are delivered from the Classification Server; you do not have to configure individual message classes for journal archiving.)

Message/Email Properties and Attributes condition parameters **Table 27-3** (continued)

MAPI Attribute	Description
Also Match	Select this option to create a compound rule. All conditions must match for the rule to trigger an incident. You can add any available condition from the drop-down menu.
	<b>Note:</b> Exchange messages that are delivered from a Classification Server do not include envelope information.
	See "Detection messages and message components" on page 305.
	See "Selecting components to match on" on page 336.

# Detecting network and mobile incidents

This chapter includes the following topics:

- Introducing protocol monitoring for network
- Introducing protocol monitoring for mobile
- Configuring the Protocol Monitoring condition for network detection
- Configuring the Protocol Monitoring condition for mobile detection
- Best practices for using network protocol matching

# Introducing protocol monitoring for network

Symantec Data Loss Prevention provides the Protocol Monitoring condition which lets you detect network messages based on the communications transport method.

Table 28-1 lists the protocols that Data Loss Prevention supports for network detection.

**Table 28-1** Supported protocols for network monitoring

Protocol	Description
Email/SMTP	Simple Mail Transfer Protocol (SMTP) is a protocol for sending email messages between servers.
FTP	The file transfer protocol (FTP) is used on the Internet for transferring files from one computer to another.
НТТР	The hypertext transfer protocol (HTTP) is the underlying protocol that supports the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

Protocol	Description
HTTP/SSL	Hypertext transfer protocol over Secure Sockets Layer (HTTPS) is a protocol for sending data securely between a client and server.
IM:MSN IM:AIM IM:AIM	Instant messaging is a type of communications service that enables you to create a private chat room with another individual.  Data Loss Prevention supports detection on the following IM channels.:  AIM instant messaging  MSN instant messaging  Yahoo! Instant messaging
NNTP	Network News Transport Protocol (NNTP), which is used to send, distribute, and retrieve USENET messages.
TCP:custom_protocol	The Transmission Control Protocol (TCP) is used to reliably exchange data between computers across the Internet. This option is only available if you have defined a custom TCP port.

**Table 28-1** Supported protocols for network monitoring (continued)

See "Configuring the Protocol Monitoring condition for network detection" on page 628.

See "Introducing protocol monitoring for mobile" on page 627.

## Introducing protocol monitoring for mobile

Symantec Data Loss Prevention provides the Protocol Monitoring condition which lets you detect mobile messages based on the communications transport method.

Table 28-2 lists the protocols that Data Loss Prevention supports for mobile detection.

**Table 28-2** Supported protocols for mobile monitoring

Protocol	Description
FTP	File transfer protocol (FTP) is used on the Internet for transferring files from one computer to another.
HTTP	The hypertext transfer protocol (HTTP) is the underlying protocol that supports the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
HTTP/SSL	Hypertext transfer protocol over Secure Sockets Layer (HTTPS) is a protocol for sending data securely between a client and server.

See "Introducing protocol monitoring for network" on page 626.

See "Configuring the Protocol Monitoring condition for mobile detection" on page 629.

#### **Configuring the Protocol Monitoring condition for** network detection

You use the Protocol Monitoring condition to detect network incidents. You can implement an instance of the Protocol Monitoring condition in one or more policy detection rules and exceptions.

Protocol Monitoring condition parameters for Network Table 28-3

Table 20-5 Protocol Monitoring condition parameters for Network		
Action	Description	
Add or modify the Protocol or Endpoint Monitoring	Add a new <b>Protocol or Endpoint Monitoring</b> condition to a policy rule or exception, or modify an existing rule or exception condition.	
condition.	See "Configuring policies" on page 326.	
	See "Configuring policy rules" on page 330.	
	See "Configuring policy exceptions" on page 340.	
Select one or more	To detect Network incidents, select one or more Protocols.	
protocols to match.	<ul> <li>Email/SMTP</li> <li>FTP</li> <li>HTTP</li> <li>HTTPS/SSL</li> <li>IM:AIM</li> <li>IM:MSN</li> <li>IM:Yahoo</li> <li>NNTP</li> </ul>	
Configure a custom network protocol.	Select one or more custom protocols: TCP:custom_protocol.	
Configure endpoint monitoring.	See "Configuring the Endpoint Monitoring condition" on page 635.	
Match on the entire message.	The Protocol Monitoring condition matches on the entire message, not individual message components.	
	The <b>Envelope</b> option is selected by default. You cannot select individual message components.	
	See "Detection messages and message components" on page 305.	

Action	Description
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

Table 28-3 Protocol Monitoring condition parameters for Network (continued)

### **Configuring the Protocol Monitoring condition for** mobile detection

You use the Protocol Monitoring condition to detect mobile incidents. You can use this condition in policy detection rules and exceptions.

Table 28-4 describes the configuration of the Protocol Monitoring condition for mobile detection.

Protocol Monitoring condition parameters for Mobile Table 28-4

Action	Description
Add or modify the Protocol or Endpoint Monitoring	Add a new <b>Protocol or Endpoint Monitoring</b> condition to a policy rule or exception, or modify an existing rule or exception condition.
condition.	See "Configuring policies" on page 326.
	See "Configuring policy rules" on page 330.
	See "Configuring policy exceptions" on page 340.
Select one or more protocols to match.	<ul> <li>To detect Mobile incidents, select one or more Protocols:</li> <li>FTP         File transfer protocol is used on the Internet for transferring files from one computer to another.     </li> <li>HTTP         The hypertext transfer protocol is the underlying protocol that supports the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.     </li> <li>HTTPS/SSL         Hypertext transfer protocol over Secure Sockets Layer, which is a protocol for sending     </li> </ul>
Custom network protocol.	data securely between a client and server.  Mobile monitoring only supports FTP, HTTP, and HTTP/S.

Action	Description
Configure endpoint monitoring.	See "Configuring the Endpoint Monitoring condition" on page 635.
Match on the entire message.	The Protocol Monitoring condition matches on the entire message, not individual message components.
	The <b>Envelope</b> option is selected by default. You cannot select individual message components.
	See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

Protocol Monitoring condition parameters for Mobile (continued) **Table 28-4** 

#### Best practices for using network protocol matching

This section provides best practices for using file property matching conditions to match file formats, file size, and file name.

#### Use separate policies for specific protocols

You can use protocol matching detection to detect network traffic, such as Web mail, social networking, and specific protocols. For protocol monitoring, consider implementing different policies for each type of protocol, such as SMTP, TCP, HTTP, FTP, etc. Creating separate policies for specific protocols may ease remediation and help you tune the policies.

#### Consider detection server network placement to support IP address matching

You can detect senders/users and recipients based one or more IP addresses. However, to do so you must carefully consider the placement of the detection server on your network.

If the detection server is installed between the Web proxy and the Internet, the IP address of all Web traffic from individuals in your organization appears to come from the Web proxy. If the detection server is installed between the Web proxy and the internal corporate network, the IP address of all Web traffic from outside your organization appears to go to the Web proxy.

The best practice is to match on domain names instead of IP addresses.

# Detecting endpoint events

This chapter includes the following topics:

- Introducing endpoint event detection
- Configuring endpoint event detection conditions
- Best practices for using endpoint detection

#### Introducing endpoint event detection

Endpoint detection matches events on endpoints where the Symantec DLP Agent is installed.

See "About Endpoint Prevent monitoring" on page 1368.

Symantec Data Loss Prevention provides several methods for detecting and excepting endpoint events, and a collection of response rules for responding to them.

See "Response rules for endpoint detection" on page 877.

#### About endpoint protocol monitoring

On the endpoint you can detect data loss based on the transport protocol, such as email (SMTP), Web (HTTP), and file transfer (FTP).

See "Configuring the Endpoint Monitoring condition" on page 635.

**Table 29-1** Supported protocols for endpoint monitoring

Protocol	Description
Email/SMTP	Simple Mail Transfer Protocol (SMTP) is a protocol for sending email messages between servers.

Protocol Description **FTP** The file transfer protocol (FTP) is used on the Internet for transferring files from one computer to another. HTTP The hypertext transfer protocol (HTTP) is the underlying protocol that supports the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. HTTP/SSL Hypertext transfer protocol over Secure Sockets Layer (HTTPS) is a protocol for sending data securely between a client and server. IM:MSN Instant messaging is a type of communications service that enables you to create a private chat room with another individual. IM:AIM Data Loss Prevention supports detection on the following IM channels.: IM:AIM AIM instant messaging MSN instant messaging Yahoo! Instant messaging

Table 29-1 Supported protocols for endpoint monitoring (continued)

#### About endpoint destination monitoring

You can also detect endpoint data loss on the destination where data is copied or moved, such as CD/DVD drive, USB device, or the clipboard.

See "Configuring the Endpoint Monitoring condition" on page 635.

**Table 29-2** Supported destinations for endpoint monitoring

Destination	Description
Local Drive	Monitor the local disk.
CD/DVD	The CD/DVD burner on the endpoint computer. This destination can be any type of third-party CD/DVD burning software.
Removable Storage Device	Detect data that is transferred to any eSATA, FireWire, or USB connected storage device.
Copy to Network Share	Detect data that is transferred to any network share or remote file access.
Printer/Fax	Detect data that is transferred to a printer or to a fax that is connected to the endpoint computer. This destination can also be print-to-file documents.
Clipboard	The Windows Clipboard used to copy and paste data between Windows applications.

#### About endpoint application monitoring

You can create exceptions for allowable use scenarios.

The DLP Agent monitors any third-party application you add and configure at the System > Agents > Application Monitoring screen.

The DLP Agent monitors applications when they access sensitive files.

See "Adding an application" on page 1506.

See "Configuring the Endpoint Monitoring condition" on page 635.

#### About endpoint location detection

You can detect or except events based on the location of the endpoint.

Using the Endpoint Location detection method, you can choose to detect incidents only when the endpoint is on or off the network.

For example, you might configure this condition to match only when users are off the corporate network because you have other rules in place for detecting network incidents. In this case implementing the Endpoint Location detection method would achieve this result.

See "Configuring the Endpoint Location condition" on page 637.

#### About endpoint device detection

Symantec Data Loss Prevention lets you detect or except specific endpoint devices based on described device metadata. You can configure a condition to allow endpoint users to copy files to a specific device class, such as USB drives from a single manufacturer.

See "Manage and add endpoint devices" on page 639.

For example, a policy author has a set of USB flash drives with serial numbers that range from 001-010. These are the only flash drives that should be allowed to access the company's endpoints. The policy administrator adds the serial number metadata into an exception of a policy so that the policy applies to all USB flash drives except for the drives with the serial number that falls into the 001-010 metadata. In this fashion the device metadata allows for only "trusted devices" to be allowed to carry company data.

See "Creating and modifying endpoint device configurations" on page 641.

The Endpoint Device Class or ID condition detects specific removable storage devices based on their definitions. Endpoint Destination parameters in the Endpoint Monitoring condition detect any removable storage device on the endpoint,

See "Configuring the Endpoint Device Class or ID condition" on page 638.

# Configuring endpoint event detection conditions

Table 29-3 describes the various methods for implementing endpoint event monitoring.

**Table 29-3** Detecting endpoint events

Endpoint match conditions	Details
Endpoint Protocol Monitoring	Detect endpoint data based on the protocol.
	See "About endpoint protocol monitoring" on page 632.
	See "Configuring the Endpoint Monitoring condition" on page 635.
Endpoint Destination	Detect endpoint data based on the destination.
Monitoring	See "About endpoint protocol monitoring" on page 632.
	See "Configuring the Endpoint Monitoring condition" on page 635.
Endpoint Application	Detect endpoint data based on the application.
Monitoring	See "About endpoint protocol monitoring" on page 632.
	See "Configuring the Endpoint Monitoring condition" on page 635.
Endpoint Device or Class ID	Detect when users move endpoint data to a specific device.
	See "About endpoint device detection" on page 634.
	See "Configuring the Endpoint Device Class or ID condition" on page 638.
Endpoint Location	Detect when the endpoint is on or off the corporate network.
	See "About endpoint location detection" on page 634.
	See "Configuring the Endpoint Location condition" on page 637.

#### Configuring the Endpoint Monitoring condition

The Endpoint Monitoring condition matches on endpoint message protocols, destinations, and applications.

You can implement an instance of the Endpoint Monitoring condition in one or more policy detection rules and exceptions.

Note: This topic does not address network protocol monitoring configuration.

See "Configuring the Protocol Monitoring condition for network detection" on page 628.

Configure the Endpoint Monitoring condition **Table 29-4** 

Action	Description
Add or modify the Endpoint Monitoring	Add a new <b>Protocol or Endpoint Monitoring</b> condition to a policy rule or exception, or modify an existing rule or exception condition.
condition.	See "Configuring policy rules" on page 330.
	See "Configuring policy exceptions" on page 340.
	See "Configuring policies" on page 326.
Select one or more endpoint protocols to match.	To detect Endpoint incidents, select one or more Endpoint Protocols:  Email/SMTP HTTP HTTPS/SSL IM:MSN IM:AIM IM:Yahoo FTP
Select one or more endpoint destinations.	See "About endpoint protocol monitoring" on page 632.  To detect when users move data on the endpoint, select one or more Endpoint Destinations:  Local Drive CD/DVD Removable Storage Device Copy to Network Share Printer/Fax
Monitor endpoint applications.	■ Clipboard  See "About endpoint protocol monitoring" on page 632.  To detect when endpoint applications access files, select the Application File Access option.
	See "About monitoring applications" on page 1503.

Action	Description
Match on the entire message.	The DLP Agent evaluates the entire message, not individual message components.
	The <b>Envelope</b> option is selected by default. You cannot select the other message components.
	See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

**Table 29-4** Configure the Endpoint Monitoring condition (continued)

#### Configuring the Endpoint Location condition

The Endpoint Location condition matches endpoint events based on the location of the endpoint computer where the DLP Agent is installed.

You can implement an instance of the Endpoint Location condition in one or more policy detection rules and exceptions.

See "Configuring policies" on page 326.

**Table 29-5** Configure the Endpoint Location detection condition

Action	Description
Add or modify the Endpoint Location condition.	Add a new <b>Endpoint Location</b> detection condition to a policy rule or exception, or modify an existing policy rule or exception.
	See "Configuring policy rules" on page 330.
	See "Configuring policy exceptions" on page 340.
Select the location to monitor.	Select one of the following endpoint locations to monitor:  Off the corporate network Select this option to detect or except events when the endpoint computer is off of the corporate network.  On the corporate network Select this option to detect or except events when the endpoint computer is on the corporate network. This option is the default selection.
	See "About endpoint location detection" on page 634.

Action	Description
Match on the entire message.	The DLP Agent evaluates the entire message, not individual message components.
	The <b>Envelope</b> option is selected by default. The other message components are not selectable.
	See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the list.
	See "Configuring compound match conditions" on page 342.

**Table 29-5** Configure the Endpoint Location detection condition (continued)

See "About endpoint location detection" on page 634.

See "Configuring the Endpoint Location condition" on page 637.

#### Configuring the Endpoint Device Class or ID condition

The Endpoint Device Class or ID condition lets you detect when users move endpoint data to specific devices.

You can implement the Endpoint Device Class or ID condition in one or more policy detection rules or exceptions.

See "Configuring policies" on page 326.

Configuring the Endpoint Device Class or ID condition **Table 29-6** 

Action	Description
Add or modify an Endpoint Device condition.	Add a new <b>Endpoint Device Class or ID</b> condition to a policy rule or exception, or modify an existing one.
	See "Configuring policy rules" on page 330.
	See "Configuring policy exceptions" on page 340.
Select one or more devices.	The condition matches when users move data from an endpoint computer to the selected device(s).
	Click Create an endpoint device to define one or more devices.
	See "Creating and modifying endpoint device configurations" on page 641.

	,
Action	Description
Match on the entire message.	The DLP Agent matches on the entire message, not individual message components.
	The <b>Envelope</b> option is selected by default. You cannot select other components.
	See "Detection messages and message components" on page 305.
Also match one or more additional conditions.	Select this option to create a compound condition. All conditions must match to trigger or except an incident.
	You can <b>Add</b> any condition available from the drop-down menu.
	See "Configuring compound match conditions" on page 342.

**Table 29-6** Configuring the Endpoint Device Class or ID condition (continued)

See "About endpoint device detection" on page 634.

See "Manage and add endpoint devices" on page 639.

#### Manage and add endpoint devices

From the **System > Agents > Endpoint Devices** screen you manage existing endpoint devices and add new ones.

See "About endpoint device detection" on page 634.

**Table 29-7** Manage endpoint devices

Action	Description
Add endpoint device.	Click <b>Add Device</b> to define a new endpoint device. Once defined the device is added to the list.
	See "Gathering endpoint device IDs" on page 640.
Modify existing endpoint device configurations.	To edit a device definition, select anywhere in the device row, or click the pencil icon.
	See "Creating and modifying endpoint device configurations" on page 641.
View configured endpoint devices.	The <b>Endpoint Devices</b> screen lists all configured endpoint devices.
	The columns display the following information:
	Device Name
	Device Description
	Device Definition (Regex)

Action	Description
Sort endpoint devices.	You can sort the endpoint device list by name, description, or definition.

**Table 29-7** Manage endpoint devices (continued)

#### Gathering endpoint device IDs

You add device metadata information to the Enforce Server and create one or more policy detection methods that detect or except the specific device instance or class of device. The system supports the regular expression syntax for defining the metadata. The system displays the device metadata at the **Incident Snapshot** screen during remediation.

See "Creating and modifying endpoint device configurations" on page 641.

The metadata the system requires to define the device instance or device class is the **Device Instance ID**. On Windows you can obtain the "Device Instance Id" from the Device Manager.

In addition, Symantec Data Loss Prevention provides the DeviceID. exe utility. You can use this utility to extract Device Instance ID strings. This utility also reports what devices the system can recognize for detection. This utility is available with the Enforce Server installation files.

See "About the Device ID utility" on page 1528.

Note: The Device Instance ID is also used by Symantec Endpoint Protection (SEP).

#### To obtain the Device Instance ID (on Windows)

- 1 Right-click My Computer.
- 2 Select Manage.
- 3 Select the **Device Manager**.
- 4 Click the plus sign beside any device to expand its list of device instances.
- Double-click the device instance. Or, right-click the device instance and select Properties.
- Look in the **Details** tab for the **Device Instance Id**.
- 7 Use the ID to create device metadata expressions. See "Creating and modifying endpoint device configurations" on page 641.

See "About endpoint device detection" on page 634.

See "Manage and add endpoint devices" on page 639.

#### Creating and modifying endpoint device configurations

You can configure one or more devices for specific endpoint detection. Once the device expressions are configured, you implement the Endpoint Device Class or ID condition in one or more policy rules or exceptions to deny or allow the use of the specific devices

See "Gathering endpoint device IDs" on page 640.

To create and modify endpoint device ID expressions

Click Add Device.

Perform this action from the **System > Agent > Endpoint Devices** screen.

- 2 Enter the **Device Name**.
- 3 Enter a **Device Desciption**.
- Enter the **Device Definition** expression.

The device definition must conform to the regular expression syntax.

See Table 29-8 on page 641.

See "About writing regular expressions" on page 598.

- Click **Save** to save the device configuration. 5
- Implement the Endpoint Device Class or ID condition in a detection rule or exception.

See "Configuring the Endpoint Device Class or ID condition" on page 638.

**Table 29-8** Example endpoint device expressions

Example device class	Expression example	
Generic USB Device	USBSTOR\\DISK&VEN_SANDISK&PROD_ULTRA_BACKUP&REV_8\.32\\3485731392112B52	
iPod generic	USBSTOR\\DISK&VEN_APPLE&PROD_IPOD&.*	
Lexar generic	USBSTOR\\DISK&VEN_LEXAR.*	
CD Drive	IDE\\DISKST9160412ASG0002SDM1\\4&F4ACADA&0&0\.0\.0	
Hard drive	USBSTOR\\DISK&VEN_MAXTOR&PROD_ONETOUCH_II&REV_023D\\B60899082H&0	
Blackberry generic	USBSTOR\\DISK&VEN_RIM&PROD_BLACKBERRY&REV.*	
Cell phone	USBSTOR\\DISK&VEN_PALM&PROD_PRE&REV_000\\FBB4B8FF4CAEFEC11 24DED689&0	

See "About endpoint device detection" on page 634.

See "Manage and add endpoint devices" on page 639.

## Best practices for using endpoint detection

When implementing endpoint match conditions, keep in mind the following considerations:

- Any detection method that executes on the endpoint matches on the entire message, not individual message components. See "Detection messages and message components" on page 305.
- The Endpoint Destination and Endpoint Location methods are specific to the endpoint computer and are not user-based. See "Distinguish synchronized DGM from other types endpoint detection" on page 659.
- You might often combine group and detection methods on the endpoint. Keep in mind that the policy language ANDs detection and group methods, whereas methods of the same type, two rules for example, are ORed. See "Policy detection execution" on page 308.

Chapter 30

# Detecting described identities

This chapter includes the following topics:

- Introducing described identity matching
- Described identity matching examples
- Configuring described identity matching policy conditions
- Best practices for using described identity matching

#### Introducing described identity matching

Described identity detection matches patterns in messages from email senders and recipients, Windows users, IM users, URL domains, and IP addresses.

See "Configuring described identity matching policy conditions" on page 644.

See "Configuring the Sender/User Matches Pattern condition" on page 645.

See "Configuring the Recipient Matches Pattern condition" on page 648.

## Described identity matching examples

Table 30-1 lists and describes some example described content matching examples.

**Table 30-1** Pattern identity matching examples

<b>Example Pattern</b>	Matches	Does Not Match
fr, cu	All SMTP email that is addressed to a .fr (France) or .cu (Cuba) addresses.	Any email that is addressed to French company with the .com extension instead of .fr.
		Any HTTP post to a .fr address through a Web-based mail application, such as Yahoo mail.
company.com	All SMTP email that is addressed to the specific domain URL, such as symantec.com.	Any SMTP email that is not addressed to the specific domain URL.
3rdlevel.company.com	All SMTP email that is addressed to the specific 3rd level domain, such as dlp.symantec.com.	Any SMTP email that is not addressed to the specific 3rd level domain.
bob@company.com	All SMTP email that is addressed to bob@company.com.	Any email not specifically addressed to bob@company.com, such as:
	All SMTP email that is addressed to BOB@COMPANY.COM (the pattern is not case-sensitive).	<ul><li>sally@company.com</li><li>robert.bob@company.com</li><li>bob@3rdlevel.company.com</li></ul>
192.168.0.*	All email, Web, or URL traffic specifically addressed to 192.168.0.[0-255].	Note: If the IP address does not match, use one or more domain URLs instead.
	This result assumes that the IP address maps to the desired domain, such as web.company.com.	
*/local/dom1/dom/dom2/dom3/Sym		
*/Sym*	addresses.	
*/dlp/qa/test/local/Sym*		

### **Configuring described identity matching policy** conditions

Table 30-2 lists and describes the two conditions that Symantec Data Loss Prevention provides for matching described identities.

See "Described identity matching examples" on page 643.

Match condition	Description
Sender/User Matches Pattern	Matches on an email address, domain address, IP address, Windows user name, or IM screen name/handle.  See "Configuring the Sender/User Matches Pattern condition" on page 645.
Recipient Matches Pattern	Matches on an email address, domain address, IP address, or newsgroup.  See "Configuring the Recipient Matches Pattern condition" on page 648.

**Table 30-2** Implementing described identity matching

#### About Reusable Sender/Recipient Patterns

You can create Reusable Sender/User and Recipient Patterns for use in your policies. Reusable Sender/Recipient Patterns make policy creation and management easier for policies using such patterns. For details about creating and using Reusable Sender/Recipient Patterns, refer to the following topics.

See "Configuring a Reusable Sender Pattern" on page 647.

See "Configuring a Reusable Recipient Pattern" on page 649.

#### Configuring the Sender/User Matches Pattern condition

The Sender/User Matches Pattern condition matches described user and message sender identities. You can use this condition in a policy detection rule or exception.

See "Introducing described identity matching" on page 643.

See "Best practices for using described identity matching" on page 650.

Configuring the Sender/User Matches Pattern condition describes the process for configuring the Sender/User Matches Pattern condition.

**Table 30-3** Configuring the Sender/User Matches Pattern condition

#### Description Action Enter one or more Sender **Email Address Pattern:** Patterns to match one or To match a specific email address, enter the full email address: more message senders. sales@symantec.com Note: The Pattern field ■ To match multiple exact email addresses, enter a comma-separated list: allows unlimited data (only john.smith@company.com, johnsmith@company.com, limited by the browser). jsmith@company.com ■ To match partial email addresses, enter one or more domain patterns: ■ Enter one or more top-level domain extensions, for example: .fr, .cu, .in, .jp ■ Enter one or more domain names, for example: company.com, symantec.com ■ Enter one or more third-level (or lower) domain names: web.company.com, mail.yahoo.com, smtp.gmail.com, dlp.security.symantec.com **Windows User Names** Enter the names of one or more Windows users, for example: john.smith, jsmith **IM Screen Name** Enter one or more IM screen names that are used in instant messaging systems, for example: john smith, jsmith IP Address Enter one or more IP addresses that map to the domain you want to match, for example: Exact IP address match, for example: 192.168.1.1 or for IPv6 fdda:c450:e808:3020:abcd:abcd:0000:5000 Wildcard match – The asterisk (\*) character can substitute for one or more fields, for example: 192.168.1.\* or 192.\*.168.\* or for IPv6 fdda:c450:e808:3:\*:\*:\*:\* Note: For IPv6, use only long format addresses.

Select a Reusable Sender Pattern

You can select a Sender Pattern that you have saved for reuse in your policies. Select Reusable Sender Pattern, then choose the pattern you want from the dropdown list.

Action	Description
Match on the entire message.	This condition matches on the entire message. The <b>Envelope</b> option is selected by default. You cannot select any other message component.
	See "Detection messages and message components" on page 305.
Also match additional conditions.	Select this option to create a compound condition. All conditions must match to trigger an incident.
	You can <b>Add</b> any available condition from the list.
	See "Configuring compound match conditions" on page 342.

Configuring the Sender/User Matches Pattern condition (continued) **Table 30-3** 

#### Configuring a Reusable Sender Pattern

If you want to use a Sender Pattern in multiple policies, configure a Reusable Sender Pattern. Reusable Sender Patterns can be selected for use in your policies from the Configure Policy - Edit Rule page. You can create, edit, and manage your Reusable Sender Patterns from the **Sender/Recipient Patterns** page. For example, if you use a Sender Pattern in 50 policies, using a Reusable Sender Pattern lets you enter the Sender Pattern a single time, then select it for each policy. In addition, if you need to update the Sender Pattern for those 50 policies, you can edit it from the Configure Reusable Sender Pattern page and your changes will be applied automatically to each policy using that pattern.

#### To configure a Reusable Sender Pattern

- 1 Take one of the following actions:
  - If you are configuring a policy with a Sender/User Matches Pattern rule, from the Manage > Policies > Policy List > Configure Policy - Edit Rule page, click Create Reusable Sender Pattern.
  - In the Enforce Server administration console, navigate to Manage > Policies > Sender/Recipient Patterns, then click Add > Sender Pattern.
- 2 In the General section on the Configure Reusable Sender Pattern page. enter a **Name** and **Description** for your Reusable Sender Pattern.
- In the Sender Pattern section, enter the User Patterns and IP Addresses as described in the "Configuring the Sender/User Matches Pattern condition table". See Table 30-3 on page 646.
- Click Save.

- 5 To edit a saved Reusable Sender Pattern, on the Manage > Policies > Sender/Recipient Patterns page, click the dropdown arrow next to the name of the pattern you want to edit, then select Edit.
- To delete a saved Reusable Sender Pattern, on the Manage > Policies > Sender/Recipient Patterns page, click the dropdown arrow next to the name of the pattern you want to delete, then select **Delete**.

Note: You cannot delete a Reusable Sender Pattern that is currently in use in any policy.

#### Configuring the Recipient Matches Pattern condition

The Recipient Matches Pattern condition matches the described identity of message recipients. You can use this condition in a policy detection rule or exception.

See "Introducing described identity matching" on page 643.

See "Define precise identity patterns to match users" on page 650.

Configuring the Recipient Matches Pattern condition defines the process for configuring the Recipient Matches Pattern condition.

Table 30-4 Recipient Matches Pattern condition parameters

Action	Description
Enter one or more Recipient Patterns to match one or more	Email Address/Newsgroup Pattern
message recipients. Separate multiple entries with commas.	Enter one or more email or newsgroup addresses to match the desired recipients.  To match specific email addresses, enter the full address, such as
<b>Note:</b> The Pattern field allows unlimited data (only limited by the browser).	sales@symantec.com. To match email addresses from a specific domain, enter the domain name only, such as symantec.com.
	IP Address
	Enter one or more IP address patterns that resolve to the domain that you want to match. You can use the asterisk (*) wildcard character for one or more fields. You can enter both IPv4 and IPv6 addresses separated by commas.
	URL Domain
	Enter one or more URL Domains to match Web-based traffic, including Web-based email and postings to a Web site. For example, if you want to prohibit the receipt of certain types of data using Hotmail, enter hotmail.com.

Table 30-4 Recipient Matches Pattern condition parameters (continued)

Action	Description	
Select a Reusable Recipient Pattern	You can select a Recipient Pattern that you have saved for reuse in your policies. Select <b>Reusable Recipient Pattern</b> , then choose the pattern you want from the dropdown list.	
Configure match counting.	Select one of the following options to specify the number of email recipients that must match:  ■ All recipients must match (Email Only) does not count a match unless ALL email message recipients match the specified pattern.  ■ At least _ recipients must match (Email Only) lets you specify the minimum number of email message recipients that must match to be counted.	
	Select one of the following options to specify how you want to count the matches:  Check for existence Reports a match count of 1 if there are one or more matches.  Count all matches Reports the sum of all matches.  See "Configuring match counting" on page 334.	
Match on the entire message.	ge. This condition matches on the entire message. The <b>Envelope</b> option is selected by default. You cannot select any other message component.  See "Detection messages and message components" on page 305.	
Also match additional conditions.	Select this option to create a compound condition. All conditions in a rule or exception must match to trigger an incident.  You can <b>Add</b> any available condition from the list.	
	See "Configuring compound match conditions" on page 342.	

### Configuring a Reusable Recipient Pattern

If you want to use a Recipient Pattern in multiple policies, configure a Reusable Recipient Pattern. Reusable Recipient Patterns can be selected for use in your policies from the Configure Policy - Edit Rule page. You can create, edit, and manage your Reusable Recipient Patterns from the Sender/Recipient Patterns page. For example, if you use a Recipient Pattern in 50 policies, using a Reusable Recipient Pattern lets you enter the Recipient Pattern a single time, then select it for each policy. In addition, if you need to update the Recipient Pattern for those 50 policies, you can edit it from the Configure Reusable Recipient Pattern page and your changes will be applied automatically to each policy using that pattern.

#### To configure a Reusable Recipient Pattern

- Take one of the following actions:
  - If you are configuring a policy with a Recipient Matches Pattern rule, from the Manage > Policies > Policy List > Configure Policy - Edit Rule page, click Create Reusable Recipient Pattern.
  - In the Enforce Server administration console, navigate to Manage > Policies > Sender/Recipient Patterns, then click Add > Recipient Pattern.
- In the General section on the Configure Reusable Recipient Pattern page, enter a Name and Description for your Reusable Recipient Pattern.
- In the Recipient Pattern section, enter the Email Addresses, IP Addresses, and **URL Domains** as described in the "Recipient Matches Pattern condition table".

See Table 30-4 on page 648.

- 4 Click Save.
- To edit a saved Reusable Recipient Pattern, on the Manage > Policies > Sender/Recipient Patterns page, click the dropdown arrow next to the name of the pattern you want to edit, then select **Edit**.
- To delete a saved Reusable Recipient Pattern, on the Manage > Policies > 6 Sender/Recipient Patterns page, click the dropdown arrow next to the name of the pattern you want to delete, then select **Delete**.

Note: You cannot delete a Reusable Recipient Pattern that is currently in use in any policy.

## Best practices for using described identity matching

This section provides considerations for implementing the Sender/User or Recipient Matches Pattern conditions in policy detection rules or exceptions. Keep in mind these considerations when you implement these conditions.

#### Define precise identity patterns to match users

Both the Sender/User and Recipient conditions match on the entire message, not individual message components. If either condition is used as an exception, a match excludes the entire message, not only the header.

See "Policy detection execution" on page 308.

For both described identity matching rules, the system implies an OR between all comma-separated list items and between all fields. For example, if any single email address among a list of email addresses matches, the condition reports (or excepts) an incident. Or, if either an email address, a domain name, or an IP address matches, the condition reports (or excepts) an incident.

See "Detection messages and message components" on page 305.

Table 30-5 describes the types of patterns you can use for described identity matching.

Table 30-5	Patterns for identity matching
------------	--------------------------------

Pattern	Sender/User Matches Pattern	Recipient Matches Pattern
Email address: full and partial	matches	matches
Domain address: top-level and subdomains	matches	matches
IP address	matches	matches
Windows user name	matches	does not match
IM screen name / handle	matches	does not match
Newsgroup patterns	does not match	matches

#### Specify email addresses exactly to improve accuracy

An email address must match exactly. For example, bob@company.com does not match bob@something.company.com. But, a domain name pattern such as company.com or something.company.com matches bob@something.company.com.

The email address field does not match the sender or recipient of a Web post. For example, the email address bob@yahoo.com does not match if Bob uses a Web browser to send or receive email. In this case, you must use the domain pattern mail.yahoo.com to match bob@yahoo.com.

## Match domains instead of IP addresses to improve accuracy

The URL Domain pattern matches HTTP traffic to particular URL domains. You do not enter the entire URL. For example, you enter mail.yahoo.com not http://www.mail.yahoo.com.

The system does not resolve URL domains to IP addresses. For example, you specify an IP address of 192.168.1.1 for a specific domain. If users access the domain URL using a Web browser, the system does not match emails that are

transmitted by the IP address. In this case, use a domain pattern instead of an IP address, such as internalmemos.com.

You can detect senders/users and recipients based one or more IP addresses. However, to do so you must carefully consider the placement of the detection server on your network. If the detection server is installed between the Web proxy and the Internet, the IP address of all Web traffic from individuals in your organization appears to come from the Web proxy. If the detection server is installed between the Web proxy and the internal corporate network, the IP address of all Web traffic from outside your organization appears to go to the Web proxy. The best practice is to match on domain names instead of IP addresses.

# Detecting synchronized identities

This chapter includes the following topics:

- Introducing synchronized Directory Group Matching (DGM)
- About two-tier detection for synchronized DGM
- Configuring User Groups
- Configuring synchronized DGM policy conditions
- Best practices for using synchronized DGM

## Introducing synchronized Directory Group Matching (DGM)

Symantec Data Loss Prevention provides synchronized Directory Group Matching (DGM) to detect data based on the exact identities of users, senders, and recipients of that data. Using synchronized DGM, you can connect the Enforce Server to a group directory server such as Microsoft Active Directory and detect users based on their directory group affiliation. For example, you may want to apply policies to staff only in the engineering department of your company, but not to staff in the human resources department. Synchronized DGM enables you to do this.

Synchronized DGM is based on a **User Group** configuration that you populate with users synchronized from your directory server. When you create a synchronized DGM policy, you reference the **User Group** in the policy. At runtime the synchronized DGM policy only applies to identities in the **User Group** reference by the policy. Or, consider an example where you you want to create a policy that applies to your everyone in your organization except the CEO. In this case you can create a **User** 

Group that contains the CEO's identity as a sole group member. You then define a policy exception that references the CEO User Group. At runtime the policy will ignore messages sent or received by the CEO.

See "User Groups" on page 292.

## About two-tier detection for synchronized DGM

On the endpoint, the Recipient based on a Directory Server Group condition requires two-tier detection for DLP Agents. The corresponding Sender/User based on a Directory Server Group condition does not require two-tier detection.

Be sure understand the implications of two-tier detection before you deploy the synchronized DGM Recipient rule to one or more endpoints.

See "Two-tier detection for DLP Agents" on page 309.

To check if two-tier detection is being used, check the

\SymantecDLP\Protect\logs\debug\FileReader.log on the Endpoint Server.

See "Troubleshooting policies" on page 353.

## **Configuring User Groups**

The Manage > Policies > User Groups screen displays configured User Groups and is the starting point for creating a new User Group. User Groups are used for implementing synchronized DGM.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

Note: User Groups can also be used with Microsoft Exchange Server Discover targets. See "Setting up scanning of Microsoft Exchange Servers" on page 1305.

#### To create or modify a User Group

- Establish a connection to the Active Directory server you want to synchronize with.
  - See "Configuring directory server connections" on page 127.
- At the Manage > Policies > User Groups screen, click Create New Group.
  - Or, to edit an existing user group, select the group in the **User Groups** screen.

3 Configure the User Group parameters as required.

See Table 31-1 on page 655.

Note: If this is the first time you are configuring the User Group, you must select the option Refresh the group directory index on Save to populate the User Group.

- After you locate the users you want, use the Add and Remove options to include or exclude them in the User Group.
- 5 Click Save.

Configure a User Group **Table 31-1** 

Action	Description
Enter the group	The <b>Group Name</b> is the name that you want to use to identify this group.
name.	Use a descriptive name so that you can easily identify it later on.
Enter the group description	Enter a short <b>Description</b> of the group.
View which policies	Initially, when you create a new User Group, the <b>Used in Policy</b> field displays <b>None</b> .
use the group.	If the User Group already exists and you modify it, the system displays a list of the policies that implement the User Group, assuming one or more group-based policies is created for this User Group.
Refresh the group directory index on Save.	Select (check) the <b>Refresh the group directory index on Save</b> option to synchronize the user group profile with the most recent directory server index immediately on <b>Save</b> of the profile. If you leave this box unselected (unchecked), the profile is synchronized with the directory server index based on the Directory Connection setting.
	See "Scheduling directory server indexing" on page 129.
	If this is the first time you are configuring the User Group profile, you must select the <b>Refresh the group directory index on Save</b> option to populate the profile with the latest directory server index replication.
Select the directory	Select the directory server you want to use from the <b>Directory Server</b> list.
server.	You must establish a connection to the directory server before you create the User Group profile.
	See "Configuring directory server connections" on page 127.

**Table 31-1** Configure a User Group (continued)

Action	Description
Search the directory for specific users.	Enter the search string in the search field and click <b>Search</b> to search the directory for specific users. You can search using literal text or wildcard characters (*).
	The search results display the Common Name (CN) and the Distinguished Name (DN) of the directory server that contains the user. These names give you the specific user identity. Results are limited to 1000 entries.
	Click Clear to clear the results and begin a new search of the directory.
	Literal text search criteria options:
	<ul> <li>Name of individual node, such as "engineering" or "accounting"</li> <li>Email address, such as "goakham@symantec-dlp.com"</li> </ul>
	Wildcard character search criteria options:
	<ul> <li>The supported wildcard character is an asterisk (*)</li> <li>Proper wildcard search examples:         <ul> <li>Gabriel *akha* returns "Gabriel Oakham"</li> <li>j* jop* returns "Janice Joplin"</li> </ul> </li> <li>Improper wildcard search:         <ul> <li>Do not begin the search string with a wildcard; this will hinder directory server search</li> </ul> </li> </ul>
	performance.
	■ For example, the following search is not recommended: *Gabriel Oakham.
Browse the directory for user groups.	You can browse the directory tree for groups and users by clicking on the individual nodes and expanding them until you see the group or node that you want.
	The browse results display the name of each node. These names give you the specific user identity.
	The results are limited to 20 entries by default. Click <b>See More</b> to view up to 1000 results.
Add a user group to	To add a group or user to the User Group profile, select it from the tree and click <b>Add</b> .
the profile.	After you select and add the node to the <b>Added Groups</b> column, the system displays the Common Name (CN) and the Distinguished Name (DN).
Save the user group.	Click <b>Save</b> to save the User Group profile you have configured.

## **Configuring synchronized DGM policy conditions**

To implement synchronized DGM policies, you define a **Directory Connection** using the Enforce Server administration console. The **Directory Connection** specifies the directory server you want to use as source information for defining exact identity **User Groups**. You then define one or more **User Groups** in the Enforce Server administration console and populate the group by synchronizing the User Group with the directory server. You then associate the User Groups with the Sender/User based on a Directory Server Group group rule or the Recipient matches User Group based on a Directory Server group rule.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

Table 31-2 describes the process for implementing synchronized DGM.

**Table 31-2** Workflow for implementing synchronized DGM

Step	Action	Description	
1	Create the connection to the directory server.	Establish the connection from the Enforce Server to a directory server such as Microsoft Active Directory.	
		See "Configuring directory server connections" on page 127.	
2	Create the User Group.	Create one or more <b>User Groups</b> on the Enforce Server and populate the <b>User Groups</b> with the exact identities from the users, groups, and business units that are defined in the directory server	
		See "Configuring User Groups" on page 654.	
3	Configure a new policy or edit an existing one.	See "Configuring policies" on page 326.	
4	Configure one or more group rules or exceptions.	Choose the type of synchronized DGM rule you want to implement and reference the <b>User Group</b> . After the policy and the group are linked, the policy applies only to those identifies in the referenced <b>User Group</b> .	
		See "Configuring the Sender/User based on a Directory Server Group condition" on page 657.	
		See "Configuring the Recipient based on a Directory Server Group condition" on page 658.	

#### Configuring the Sender/User based on a Directory Server Group condition

The condition Sender/User based on a Directory Server Group matches policy violations based on message senders and endpoint users synchronized from a directory group server. You can implement this condition in a policy group (identity) rule or exception.

See "Configuring policies" on page 326.

**Note:** If the identity being detected is a user, the user must be actively logged on to a DLP Agent-enabled system for the policy to match.

Parameter	Description	
Select User Groups to	Select one or more <b>User Groups</b> that you want this policy to detect.	
include in this policy	If you have not created a User Group, click Create a new User Group.	
	See "Configuring User Groups" on page 654.	
Match On	This condition matches on the entire message. The <b>Envelope</b> option is selected by default. You cannot select any other message component.	
	See "Detection messages and message components" on page 305.	
Also Match	Select this option to create a compound condition. All conditions in a rule or exception must match to trigger an incident.	
	You can <b>Add</b> any available condition from the list.	
	See "Configuring compound match conditions" on page 342.	

**Table 31-3** Sender/User matches User Group condition parameters

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

#### Configuring the Recipient based on a Directory Server Group condition

The Recipient based on a Directory Server Group condition matches policy violations based on specific message recipients synchronized from a directory server. You can implement this condition in a policy group rule or exception.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

Note: The Recipient based on a Directory Server Group condition requires two-tier detection. See "About two-tier detection for synchronized DGM" on page 654.

Configuring the Recipient based on a Directory Server Group Table 31-4 condition

Step	Action	Description
1	Select User Groups to	Select the User Group(s) that you want this policy to match on.
include in this policy	If you have not created a User Group, click <b>Create a new Endpoint User Group</b> option.	
		See "Configuring User Groups" on page 654.

Step	Action	Description
2	Match On	This rule detects the entire message, not individual components. The <b>Envelope</b> option is selected by default. You cannot select any other message component.  See "Detection messages and message components" on page 305.
3	Also Match	Select this option to create a compound condition. All conditions in a rule or exception must match to trigger an incident.
		You can <b>Add</b> any available condition from the list.  See "Configuring compound match conditions" on page 342.

**Table 31-4** Configuring the Recipient based on a Directory Server Group condition (continued)

## Best practices for using synchronized DGM

This section contains a few considerations to keep in mind when implementing synchronized DGM conditions in your policies.

#### Refresh the directory on initial save of the User Group

To execute a policy rule based on an Active Directory group, the index that you define on the Enforce Server must first be populated. When you first define the User Group, the recommendation is to select the option "Refresh the group directory index on Save." This ensures proper synchronization of Active Directory with the Enforce Server. Once the User Group is populated, you can then set up scheduling to keep the user group on Enforce in sync with the Active Directory server.

One use case for not indexing immediately is where you are creating multiple User Groups and you want to index after you have defined all the groups. In this case you can use scheduling, but keep in mind that any policies based on these indices will not execute until they are populated.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

See "Configuring User Groups" on page 654.

#### Distinguish synchronized DGM from other types endpoint detection

When synchronized DGM policies are deployed to endpoint servers, identity-based detection applies to the users in a configured group of DLP Agent-based endpoints. With endpoint-based user groups, many different users can log on to the same computer depending on business practices. The response that each user sees on that endpoint varies depending on how the users are grouped. Contrast this style

of endpoint detection with the **Endpoint Protocol Destination** or **Endpinot Location** methods, which are specific to the endpoint and are not user-based.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

## Detecting profiled identities

This chapter includes the following topics:

- Introducing profiled Directory Group Matching (DGM)
- About two-tier detection for profiled DGM
- Configuring Exact Data profiles for DGM
- Configuring profiled DGM policy conditions
- Best practices for using profiled DGM

## Introducing profiled Directory Group Matching (DGM)

Profiled Directory Group Matching (DGM) leverages Exact Data Matching (EDM) technology to detect identities that you have indexed from your database or directory server using an Exact Data Profile. For example, you can use profiled DGM to identify network user activity or to analyze content associated with particular users, senders, or recipients. Or, you can exclude certain email addresses from analysis. Or, you might want to prevent certain people from sending confidential information by email.

See "Configuring Exact Data profiles for DGM" on page 662.

Profiled DGM is distinguished from synchronized DGM, which uses a connection to a directory server (such as Microsoft Active Directory) to match identities.

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

## About two-tier detection for profiled DGM

Profiled DGM relies on an EDM index, which is server-based. Profiled DMG requires two-tier detection for DLP Agents on the endpoint.

See "About two-tier detection for EDM on the endpoint" on page 377.

You cannot combine either type of profiled DGM condition with an Endpoint: Block or **Endpoint: Notify** response rule in a policy. If you do, the system reports that the policy is misconfigured.

See "Troubleshooting policies" on page 353.

## **Configuring Exact Data profiles for DGM**

To implement profiled DGM, you export identity records from a directory server or database, index the data, and create an Exact Data Profile. You then reference this profile in the corresponding Sender/User or Recipient condition.

See "Introducing profiled Directory Group Matching (DGM)" on page 661.

Table 32-1 describes the procedure for configuring Exact Data profiles for DGM policies.

<b>Table 32-1</b> Wo	orkflow for	implementing	profiled DGM
----------------------	-------------	--------------	--------------

Step	Action	Description
1	Create the data source file.	Create a data source file from the directory server or database you want to profile. Make sure the data source file contains the appropriate fields.  The following fields are supported for profiled DGM:  Email address  IP address  Window user name (in the format domain\user)  IM screen name  See "Creating the exact data source file for profiled DGM" on page 380.
2	Prepare the data source file for indexing.	See "Configuring Exact Data profiles" on page 378.  See "Preparing the exact data source file for indexing" on page 381.
3	Create the Exact Data Profile.	This includes uploading the data source file to the Enforce Server, mapping the data fields, and indexing the data source.  See "Uploading exact data source files to the Enforce Server" on page 383.  See "Creating and modifying Exact Data Profiles" on page 385.
		See "Mapping Exact Data Profile fields" on page 389.  See "Scheduling Exact Data Profile indexing" on page 392.

Step	Action	Description
4	Define the profiled DGM condition.	See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.
		See "Configuring the Recipient based on a Profiled Directory condition" on page 664.
5	Test the profiled DGM policy.	Use a test policy group and verify that the matches the policy generates are accurate.
		See "Test and tune policies to improve match accuracy" on page 361.

Table 32-1 Workflow for implementing profiled DGM (continued)

## Configuring profiled DGM policy conditions

Symantec Data Loss Prevention provides two match conditions for profiled DGM: sender/user and recipient. Both conditions can be used as policy rules or exceptions. For example, consider a scenario where you index a list of email addresses and author profiled DGM policies based on this indexed data. You could write a rule that requires the message sender to be from the indexed list to violate the policy. Or, you could write an exception that is not violated if the recipient of an email is from the indexed list.

See "Creating the exact data source file for profiled DGM" on page 380.

Table 32-2	Profiled DGM co	nditions

Group rule	Description
Sender/User based on a Directory from <edm profile=""></edm>	If this condition is implemented as a policy rule, a match occurs only if the sender or user of the data is contained in the index profile. If this condition is implemented as a policy exception, the data will be excepted from matching if it is sent by a sender/user listed in the index profile
Recipient based on a Directory from <edm profile=""></edm>	If this condition is implemented as a policy rule, a match occurs only if the recipient of the data is contained in the index profile. If this condition is implemented as a policy exception, the data will be excepted from matching if it is received by a recipient listed in the index profile.

#### Configuring the Sender/User based on a Profiled Directory condition

The Sender/User based on a Directory from detection rule lets you create detection rules based on sender identity or (for endpoint incidents) user identity. This condition requires an Exact Data Profile.

See "Creating the exact data source file for profiled DGM" on page 380.

After you select the Exact Data Profile, when you configure the rule, the directory you selected and the sender identifier(s) appear at the top of the page.

Table 32-3 describes the parameters for configuring the Sender/User based on a **Directory an EDM Profile** condition.

Configuring the Sender/User based on a Directory from an EDM **Table 32-3** Profile condition

Parameter	Description
Where	Select this option to have the system match on the specified field values. Specify the values by selecting a field from the drop-down list and typing the values for that field in the adjacent text box. If you enter more than one value, separate the values with commas.
	For example, for an Employees directory group profile that includes a <b>Department</b> field, you would select <b>Where</b> , select <b>Department</b> from the drop-down list, and enter <b>Marketing,Sales</b> in the text box. If the condition is implemented as a rule, in this example a match occurs only if the sender or user works in Marketing or Sales (as long as the other input content meets all other detection criteria). If the condition is implemented as an exception, in this example the system ignores from matching messages from a sender or user who works in Marketing or Sales.
Is Any Of	Enter or modify the information you want to match. For example, if you want to match any sender in the Sales department, select <b>Department</b> from the drop-down list, and then enter <b>Sales</b> in this field (assuming that your data includes a Department column). Use a comma-separated list if you want to specify more than one value.

#### Configuring the Recipient based on a Profiled Directory condition

The Recipient based on a Directory from condition lets you create detection methods based on the identity of the recipient. This method requires an Exact Data Profile.

See "Creating the exact data source file for profiled DGM" on page 380.

After you select the Exact Data Profile, when you configure the rule, the directory you selected and the recipient identifier(s) appear at the top of the page.

Table 32-3 describes the parameters for configuring Recipient based on a Directory from an EDM profile condition.

Configuring the Recipient based on a Directory from an EDM profile **Table 32-4** condition

Parameter	Description
Where	Select this option to have the system match on the specified field values. Specify the values by selecting a field from the drop-down list and typing the values for that field in the adjacent text box. If you enter more than one value, separate the values with commas.
	For example, for an Employees directory group profile that includes a <b>Department</b> field, you would select <b>Where</b> , select <b>Department</b> from the drop-down list, and enter <b>Marketing</b> , <b>Sales</b> in the text box. For a detection rule, this example causes the system to capture an incident only if at least one recipient works in Marketing or Sales (as long as the input content meets all other detection criteria). For an exception, this example prevents the system from capturing an incident if at least one recipient works in Marketing or Sales.
Is Any Of	Enter or modify the information you want to match. For example, if you want to match any recipient in the Sales department, select <b>Department</b> from the drop-down list, and then enter <b>Sales</b> in this field (assuming that your data includes a Department column). Use a comma-separated list if you want to specify more than one value.

## Best practices for using profiled DGM

Keep in mind the considerations in this section when implementing profiled Directory Group Matching (DGM)

#### Follow EDM best practices when implementing profiled DGM

Profiled DGM leverages EDM technology. Follow the EDM procedures and best practices when implementing profiled DGM.

See "About two-tier detection for profiled DGM" on page 661.

#### Include an email address field in the Exact Data Profile for profiled **DGM**

You must include the appropriate fields in the Exact Data Profile to implement profiled DGM.

See "Creating the exact data source file for profiled DGM" on page 380.

If you include the email address field in the Exact Data Profile for profiled DGM and map it to the email data validator, email address will appear in the Directory EDM drop-down list (at the remediation page).

### Use profiled DGM for Network Prevent for Web identity detection

If you want to implement DGM for Network Prevent for Web, use one of the profiled DGM conditions to implement identity matching. For example, you may want to use identity matching to block all web traffic for a specific users. For Network Prevent for Web, you cannot use synchronized DGM conditions for this use case.

See "Creating the exact data source file for profiled DGM" on page 380.

See "Configuring the Sender/User based on a Profiled Directory condition" on page 663.

# Supported file formats for detection

This chapter includes the following topics:

- Overview of detection file format support
- Supported formats for file type identification
- Supported formats for content extraction
- Supported encapsulation formats for subfile extraction
- Supported file formats for metadata extraction

## Overview of detection file format support

Symantec Data Loss Prevention detection supports various file formats for performing the following operations:

- File type identification
- File contents extraction
- Subfile extraction
- Document metadata extraction

Table 33-1 summarizes the file formats that Symantec Data Loss Prevention supports for file type identification and content, subfile and metadata extraction.

You configure the system to identify individual file formats using the **Message Attachment or File Type Match** condition. This condition performs a context-based match that only identifies the file format type; it does not extract file contents. In addition, you must explicitly select the individual file format(s) you want to detect.

See "About file type matching" on page 609.

When you use a content-based detection condition in a policy (such as Content Matches Keyword), the system automatically extracts file contents for supported file formats (such as DOCX, PPTX, XSLX, PDF). In addition, the system automatically extracts subfiles from supported encapsulation file formats (such as ZIP, RAR, TAR).

See "Content matching conditions" on page 301.

Lastly, you can enable metadata extraction for a limited number of document formats (such as DOCX), and use keyword matching to detect document metadata.

See "About document metadata detection" on page 693.

Note: While there is some overlap among file types supported for extraction and for identification (because if the system can can crack the file it must be able to identify its type), the supported formats for each operation are distinct and implemented using different match conditions. The number of file formats supported for type identification is much broader than those supported for content extraction.

Table 33-1 File format support for detection operations

Operation type	Description	Configuration	Supported formats
File type identification	Symantec Data Loss Prevention does not rely on file extensions to identify the format. File type is identified by the unique binary signature of the file format.	Explicitly using the Message Attachment or File Type Match file property condition.	See "Supported formats for file type identification" on page 669.
File contents extraction	File contents is any text-based content that can be viewed through the native or source application.	Implicitly using one or more content match conditions, including EDM, IDM, VML, data identifiers, keyword, regular expressions.	See "Supported formats for content extraction" on page 684.
Subfile extraction (Subfile)	Subfiles are files encapsulated in a parent file. Subfiles are extracted and processed individually for identification and content extraction. If the subfile format is not supported by default, a custom method can be used to detect and crack the file.	Implicitly using one or more content match conditions, including EDM, IDM, VML, data identifiers, keyword, regular expressions.	See "Supported encapsulation formats for subfile extraction" on page 691.

Operation type	Description	Configuration	Supported formats
Metadata extraction (Metadata)	Metadata is information about the file, such as author, version, or user-defined tags. Generally limited to Microsoft Office documents (OLE-enabled) and Adobe PDF files. Metadata support may differ between agent and server.	Available for content-based match conditions. Must be enabled.	See "Supported file formats for metadata extraction" on page 692.

Table 33-1 File format support for detection operations (continued)

## Supported formats for file type identification

Table 33-2 lists the file types you can identify using the Message Attachment or File Type Match policy condition.

See "About file type matching" on page 609.

If the file format you want to identify is not supported, you can use the Symantec Data Loss Prevention Scripting Language to identify custom file types.

See "About custom file type identification" on page 610.

Note: The Message Attachment or File Type Match condition is a context-based match condition that only supports file type identification. This condition does not support file contents extraction. To extract file contents for policy evaluation you must use a content-based detection rule. See "Supported formats for content extraction" on page 684.

See "Overview of detection file format support" on page 667.

**Table 33-2** Formats supported for file type identification

Message Attachment or File Type Match formats	
7-Zip Compressed File (7Z)	
Ability Office (SS)	
Ability Office (DB)	
Ability Office (GR)	
Ability Office (WP)	
Ability Office (COM)	

Message Attachment or File Type Match formats
ACT
Adobe FrameMaker
Adobe Maker Interchange Format (FrameMaker)
Adobe FrameMaker Markup Language
Adobe PDF
AES Multiplus Comm
Aldus Freehand (Macintosh)
Aldus PageMaker (DOS)
Aldus PageMaker (Macintosh)
Amiga IFF-8SVX sound
Amiga MOD sound
ANSI
Apple Double
Apple Single
Applix Alis
Applix Asterix
Applix Graphics
Applix Presents
Applix Spreadsheets
Applix Words
ARC/PAK Archive
ASCII
ASCII-armored PGP encoded
ASCII-armored PGP Public Keyring
ASCII-armored PGP signed

Message Attachment or File Type Match formats
Audio Interchange File Format
AutoCAD Drawing
AutoCAD Drawing Exchange
AutoDesk Animator FLIC Animation
AutoDesk Animator Pro FLIC Animation
AutoDesk WHIP
AutoShade Rendering
BinHex
CADAM Drawing (CDD) (server only)
CADAM Drawing Overlay
CATIA Drawing (CAT) (server only)
CCITT Group 3 1-Dimensional (G31D)
COMET TOP Word
Comma Separated Values
Compactor/Compact Pro Archive
Computer Graphics Metafile
Convergent Tech DEF Comm.
Corel Draw CMX
Corel Presentations
Corel Quattro Pro (WB2)
Corel Quattro Pro (WB3)
Corel WordPerfect Linux
Corel WordPerfect Macintosh
Corel WordPerfect Windows (WO)
Corel WordPerfect Windows (WPD)

Message Attachment or File Type Match formats
CorelDRAW
cpio Archive (UNIX)
cpio Archive (VAX)
cpio Archive (SUN)
CPT Communication
Creative Voice (VOC) sound
Curses Screen Image (UNIX)
Curses Screen Image (VAX)
Curses Screen Image (SUN)
Data Interchange Format
Data Point VISTAWORD
dBase Database
DCX Fax
DCX Fax System
DEC WPS PLUS
DECdx
Desktop Color Separation (DCS)
Device Independent file (DVI)
DG CEOwrite
DG Common Data Stream (CDS)
DIF Spreadsheet
Digital Document Interchange Format (DDIF)
Disk Doubler Compression
DisplayWrite
Domino XML Language

ENABLE ENABLE Spreadsheet (SSF) Encapsulated PostScript (raster) Enhanced Metafile Envoy (EVY) Executable- Other Executable- UNIX Executable- UNIX Executable- SUN ElieMaker (Macintosh) Elie Share Encryption Folio Flat File Framework Framework Framework II ETTP Session Data Fujitsu Oasys SEM Bit Image GIF Graphics Environment Manager (GEM VDI) SZIP Haansoft Hangul (Hangul 2010 SE+)	Message Attachment or File Type Match formats
ENABLE Spreadsheet (SSF) Encapsulated PostScript (raster) Enhanced Metafile Envoy (EVY) Executable- Other Executable- UNIX Executable- UNIX Executable- SUN FileMaker (Macintosh) File Share Encryption Folio Flat File Framework Framework II ETP Session Data Eujitsu Oasys SEM Bit Image GIF Graphics Environment Manager (GEM VDI) SZIP Haansoft Hangul (Hangul 2010 SE+)	EBCDIC Text
EnABLE Spreadsheet (SSF) Encapsulated PostScript (raster) Enhanced Metafile Envoy (EVY) Executable- Other Executable- UNIX Executable- VAX Executable- SUN FileMaker (Macintosh) File Share Encryption Folio Flat File Framework Framework II ETP Session Data Fujitsu Oasys GEM Bit Image SIF Graphics Environment Manager (GEM VDI) SZIP Haansoft Hangul (Hangul 2010 SE+)	EMC EmailXtender Container File (EMX)
Encapsulated PostScript (raster) Enhanced Metafile Envoy (EVY) Executable- Other Executable- UNIX Executable- VAX Executable- SUN File Maker (Macintosh) File Share Encryption Folio Flat File Framework Framework II FTP Session Data Fujitsu Oasys SEM Bit Image SIF Graphics Environment Manager (GEM VDI) SZIP Haansoft Hangul (Hangul 2010 SE+)	ENABLE
Enhanced Metafile Envoy (EVY) Executable- Other Executable- UNIX Executable- VAX Executable- SUN FileMaker (Macintosh) File Share Encryption Folio Flat File Framework Framework Framework II FTP Session Data Fujitsu Oasys GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	ENABLE Spreadsheet (SSF)
Envoy (EVY)  Executable- Other  Executable- UNIX  Executable- VAX  Executable- SUN  FileMaker (Macintosh)  File Share Encryption  Folio Flat File  Framework  Framework II  FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Encapsulated PostScript (raster)
Executable- Other  Executable- UNIX  Executable- VAX  Executable- SUN  FileMaker (Macintosh)  File Share Encryption  Folio Flat File  Framework  Framework II  FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Enhanced Metafile
Executable- UNIX Executable- VAX Executable- SUN FileMaker (Macintosh) File Share Encryption Folio Flat File Framework Framework Framework II FTP Session Data Fujitsu Oasys GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	Envoy (EVY)
Executable- VAX  Executable- SUN  FileMaker (Macintosh)  File Share Encryption  Folio Flat File  Framework  Framework II  FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Executable- Other
Executable- SUN  FileMaker (Macintosh)  File Share Encryption  Folio Flat File  Framework  Framework  Framework II  FTP Session Data  Fujitsu Oasys  SEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  SZIP  Haansoft Hangul (Hangul 2010 SE+)	Executable- UNIX
File Maker (Macintosh) File Share Encryption Folio Flat File Framework Framework II FTP Session Data Fujitsu Oasys GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	Executable- VAX
File Share Encryption Folio Flat File Framework Framework II FTP Session Data Fujitsu Oasys GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	Executable- SUN
Framework Framework II FTP Session Data Fujitsu Oasys GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	FileMaker (Macintosh)
Framework II  FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	File Share Encryption
Framework II  FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Folio Flat File
FTP Session Data  Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Framework
Fujitsu Oasys  GEM Bit Image  GIF  Graphics Environment Manager (GEM VDI)  GZIP  Haansoft Hangul (Hangul 2010 SE+)	Framework II
GEM Bit Image GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	FTP Session Data
GIF Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	Fujitsu Oasys
Graphics Environment Manager (GEM VDI) GZIP Haansoft Hangul (Hangul 2010 SE+)	GEM Bit Image
GZIP Haansoft Hangul (Hangul 2010 SE+)	GIF
Haansoft Hangul (Hangul 2010 SE+)	Graphics Environment Manager (GEM VDI)
	GZIP
Harvard Graphics	Haansoft Hangul (Hangul 2010 SE+)
	Harvard Graphics
Hewlett-Packard	Hewlett-Packard

Message Attachment or File Type Match formats
Honey Bull DSA101
HP Graphics Language (HPG) (server only)
HP Printer Control Language (PCL)
HTML
IBM 1403 Line Printer
IBM DCA/RFT(Revisable Form Text)
IBM DCA-FFT
IBM DCF Script
Informix SmartWare II
Informix SmartWare II Communication File
Informix SmartWare II Database
Informix SmartWare Spreadsheet
Interleaf
Java Archive
JPEG
JPEG File Interchange Format (JFIF)
JustSystems Ichitaro
KW ODA G31D (G31)
KW ODA G4 (G4)
KW ODA Internal G32D (G32)
KW ODA Internal Raw Bitmap (RBM)
Lasergraphics Language
Legato Extender
Link Library- Other
Link Library UNIX

Message Attachment or File Type Match formats
Link Library VAX
Link Library SUN
Lotus 1-2-3 (123)
Lotus 1-2-3 (WK4)
Lotus 1-2-3 Charts
Lotus AMI Pro
Lotus AMI Professional Write Plus
Lotus AMIDraw Graphics
Lotus Freelance Graphics
Lotus Freelance Graphics 2
Lotus Notes Bitmap
Lotus Notes CDF
Lotus Notes database
Lotus Pic
Lotus Screen Cam
Lotus SmartMaster
Lotus Word Pro
Lyrix MacBinary
MacBinary
Macintosh Raster
MacPaint
Macromedia (Adobe) Director
Macromedia (Adobe) Flash
MacWrite
MacWrite II

Table 33-2 Torniats supported for the type identification (continued)
Message Attachment or File Type Match formats
MASS-11
Micrografx Designer
Microsoft Access
Microsoft Advanced Systems Format (ASF)
Microsoft Compressed Folder (LZH)
Microsoft Compressed Folder (LHA)
Microsoft Device Independent Bitmap
Microsoft Excel Charts
Microsoft Excel Macintosh
Microsoft Excel Windows
Microsoft Excel Windows XML
Microsoft Office Access (ACCDB)
Microsoft Office Drawing
Microsoft OneNote
Microsoft Outlook Personal Folder
Microsoft Outlook
Microsoft Outlook Express
Microsoft PowerPoint Macintosh
Microsoft PowerPoint PC
Microsoft PowerPoint Windows
Microsoft PowerPoint Windows XML
Microsoft PowerPoint Windows Macro-Enabled XML
Microsoft PowerPoint Windows XML Template
Microsoft PowerPoint Windows Macro-Enabled XML Template
Microsoft PowerPoint Windows XML Show

Microsoft Project Microsoft Publisher Microsoft Visio Microsoft Visio XML Microsoft Wave Sound Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Les Encapsulation Microsoft Windows OLE 2 Encapsulation Microsoft Windows Virite Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh) Microsoft Works Database (PC)	Message Attachment or File Type Match formats
Microsoft Publisher Microsoft Visio Microsoft Visio XML Microsoft Wave Sound Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word Windows Write Microsoft Word Windows Write Microsoft Word Windows Macro-Enabled Template XML Microsoft Word Windows Amaro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Communication (Windows) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft PowerPoint Windows Macro-Enabled Show
Microsoft Visio Microsoft Visio XML Microsoft Wave Sound Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word Windows Write Microsoft Word Windows Write Microsoft Word Windows Wile Microsoft Word Windows Microsoft Word PC Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Project
Microsoft Visio XML Microsoft Wave Sound Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Loon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Publisher
Microsoft Wave Sound Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works Communication (Macintosh) Microsoft Works Database (Macintosh)	Microsoft Visio
Microsoft Windows Cursor (CUR) Graphics Microsoft Windows Group File Microsoft Windows Help File Microsoft Windows Loon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word PC Microsoft Word Windows Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Visio XML
Microsoft Windows Help File Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word PC Microsoft Word Windows XML Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Wave Sound
Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Windows Cursor (CUR) Graphics
Microsoft Windows Icon (ICO) Microsoft Windows OLE 2 Encapsulation Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word PC Microsoft Word Windows Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Hacro-Enabled Template XML Microsoft Words (Macintosh) Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Windows Group File
Microsoft Windows Write Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word PC Microsoft Word Windows Microsoft Word Windows Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Windows Help File
Microsoft Windows Write  Microsoft Word (UNIX)  Microsoft Word Macintosh  Microsoft Word PC  Microsoft Word Windows  Microsoft Word Windows XML  Microsoft Word Windows Template XML  Microsoft Word Windows Macro-Enabled Template XML  Microsoft Words (Macintosh)  Microsoft Works (Macintosh)  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Windows Icon (ICO)
Microsoft Word (UNIX) Microsoft Word Macintosh Microsoft Word PC Microsoft Word Windows Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Windows OLE 2 Encapsulation
Microsoft Word PC  Microsoft Word Windows  Microsoft Word Windows XML  Microsoft Word Windows Template XML  Microsoft Word Windows Macro-Enabled Template XML  Microsoft Works (Macintosh)  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Windows Write
Microsoft Word Windows Microsoft Word Windows XML Microsoft Word Windows Template XML Microsoft Word Windows Macro-Enabled Template XML Microsoft Works (Macintosh) Microsoft Works (Macintosh) Microsoft Works Communication (Macintosh) Microsoft Works Communication (Windows) Microsoft Works Database (Macintosh)	Microsoft Word (UNIX)
Microsoft Word Windows XML  Microsoft Word Windows Template XML  Microsoft Word Windows Macro-Enabled Template XML  Microsoft Works (Macintosh)  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word Macintosh
Microsoft Word Windows XML  Microsoft Word Windows Template XML  Microsoft Word Windows Macro-Enabled Template XML  Microsoft Works (Macintosh)  Microsoft Works  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word PC
Microsoft Word Windows Template XML  Microsoft Word Windows Macro-Enabled Template XML  Microsoft Works (Macintosh)  Microsoft Works  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word Windows
Microsoft Word Windows Macro-Enabled Template XML  Microsoft Works (Macintosh)  Microsoft Works  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word Windows XML
Microsoft Works (Macintosh)  Microsoft Works  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word Windows Template XML
Microsoft Works  Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Word Windows Macro-Enabled Template XML
Microsoft Works Communication (Macintosh)  Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Works (Macintosh)
Microsoft Works Communication (Windows)  Microsoft Works Database (Macintosh)	Microsoft Works
Microsoft Works Database (Macintosh)	Microsoft Works Communication (Macintosh)
	Microsoft Works Communication (Windows)
Microsoft Works Database (PC)	Microsoft Works Database (Macintosh)
	Microsoft Works Database (PC)

Message Attachment or File Type Match formats
Microsoft Works Database (Windows)
Microsoft Works Spreadsheet (S30)
Microsoft Works Spreadsheet (S40)
Microsoft Works Spreadsheet (Macintosh)
Microstation
MIDI
MORE Database Outliner (Macintosh)
MPEG-1 Audio layer 3
MPEG-1 Video
MPEG-2 Audio
MS DOS Batch File format
MS DOS Device Driver
MultiMate 4.0
Multiplan Spreadsheet
Navy DIF
NBI Async Archive Format
NBI Net Archive Format
Netscape Bookmark file
NeWS font file (SUN)
NeXT/Sun Audio
NIOS TOP
Nota Bene
Nurestor Drawing (NUR) (server only)
Oasis Open Document Format (ODT)
Oasis Open Document Format (ODS)

Message Attachment or File Type Match formats
Oasis Open Document Format (ODP)
Object Module UNIX
Object Module VAX
Object Module SUN
ODA/ODIF
ODA/ODIF (FOD 26)
Office Writer
OLE DIB object
OLIDIF
OmniOutliner (OO3)
OpenOffice Calc (SXC)
OpenOffice Calc (ODS)
OpenOffice Impress (SXI)
OpenOffice Impress (SXP)
OpenOffice Impress (ODP)
OpenOffice Writer (SXW)
OpenOffice Writer (ODT)
Open PGP
OS/2 PM Metafile Graphics
Paradox (PC) Database
PC COM executable
PC Library Module
PC Object Module
PC PaintBrush
PC True Type Font

Message Attachment or File Type Match formats
PCD Image
PeachCalc Spreadsheet
Persuasion Presentation
PEX Binary Archive (SUN)
PGP Compressed Data
PGP Encrypted Data
PGP Public Keyring
PGP Secret Keyring
PGP Signature Certificate
PGP Signed and Encrypted Data
PGP Signed Data
Philips Script
PKZIP
Plan Perfect
Portable Bitmap Utilities (PBM)
Portable Greymap Utilities (PGM)
Portable Network Graphics
Portable Pixmap Utilities (PPM)
PostScript File
PRIMEWORD
Program Information File
Q & A for DOS
Q & A for Windows
Quadratron Q-One (V1.93J)
Quadratron Q-One (V2.0)

QuickDraw 3D Metafile (3DMF) QuickTime Movie RAR archive Real Audio Reflex Database Rich Text Format RIFF Device Independent Bitmap RIFF MIDI RIFF Mildlimedia Movie SAMNA Word IV Serialized Object Format (SOF) Encapsulation SGI RGB Image SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (ODT) Sturf It Archive (Macintosh)	Message Attachment or File Type Match formats
QuickTime Movie RAR archive Real Audio Reflex Database Rich Text Format RIFF Device Independent Bitmap RIFF MIDI RIFF Miltimedia Movie SAMNA Word IV Serialized Object Format (SOF) Encapsulation SGI RGB Image SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (ODT)	Quark Express (Macintosh)
RAR archive Real Audio Reflex Database Rich Text Format RIFF Device Independent Bitmap RIFF MIDI RIFF Miltimedia Movie SAMNA Word IV Serialized Object Format (SOF) Encapsulation SGI RGB Image SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (SXC) StarOffice Palc (DDS) StarOffice Impress (SXP) StarOffice Impress (SXP) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (CDT)	QuickDraw 3D Metafile (3DMF)
Real Audio Reflex Database Rich Text Format RIFF Device Independent Bitmap RIFF MIDI RIFF MIDI RIFF Multimedia Movie SAMNA Word IV Serialized Object Format (SOF) Encapsulation SGI RGB Image SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (DS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (SXW) StarOffice Writer (CDT)	QuickTime Movie
Reflex Database Rich Text Format RIFF Device Independent Bitmap RIFF MIDI RIFF Multimedia Movie SAMNA Word IV Serialized Object Format (SOF) Encapsulation SGI RGB Image SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (SXC) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (SXW)	RAR archive
Rich Text Format  RIFF Device Independent Bitmap  RIFF MIDI  RIFF Multimedia Movie  SAMNA Word IV  Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	Real Audio
RIFF Device Independent Bitmap  RIFF MIDI  RIFF Multimedia Movie  SAMNA Word IV  Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (SXW)	Reflex Database
RIFF MIDI RIFF Multimedia Movie  SAMNA Word IV Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML Simple Vector Format (SVF)  SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (SXC) StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	Rich Text Format
RIFF Multimedia Movie  SAMNA Word IV  Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	RIFF Device Independent Bitmap
SAMNA Word IV  Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	RIFF MIDI
Serialized Object Format (SOF) Encapsulation  SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	RIFF Multimedia Movie
SGI RGB Image  SGML  Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	SAMNA Word IV
SGML Simple Vector Format (SVF) SMTP document SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW) StarOffice Calc (SXC) StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	Serialized Object Format (SOF) Encapsulation
Simple Vector Format (SVF)  SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	SGI RGB Image
SMTP document  SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	SGML
SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)  StarOffice Calc (SXC)  StarOffice Calc (ODS)  StarOffice Impress (SXI)  StarOffice Impress (SXP)  StarOffice Impress (ODP)  StarOffice Writer (SXW)  StarOffice Writer (ODT)	Simple Vector Format (SVF)
StarOffice Calc (SXC) StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	SMTP document
StarOffice Calc (ODS) StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)
StarOffice Impress (SXI) StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	StarOffice Calc (SXC)
StarOffice Impress (SXP) StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	StarOffice Calc (ODS)
StarOffice Impress (ODP) StarOffice Writer (SXW) StarOffice Writer (ODT)	StarOffice Impress (SXI)
StarOffice Writer (SXW) StarOffice Writer (ODT)	StarOffice Impress (SXP)
StarOffice Writer (ODT)	StarOffice Impress (ODP)
	StarOffice Writer (SXW)
Stuff It Archive (Macintosh)	StarOffice Writer (ODT)
	Stuff It Archive (Macintosh)

Table 33 2 Torrides supported for the type identification (continued)
Message Attachment or File Type Match formats
Sun Raster Image
SUN vfont definition
Supercalc Spreadsheet
SYLK Spreadsheet
Symphony Spreadsheet
Tagged Image File
Tape Archive
Targon Word (V 2.0)
Text Mail (MIME)
Transmission Neutral Encapsulation Format
Truevision Targa
Ultracalc Spreadsheet
Unicode Text
Uniplex (V6.01)
Uniplex Ucalc Spreadsheet
UNIX Compress
UNIX SHAR Encapsulation
Usenet format
UUEncoding
Volkswriter
VRML
Wang Office GDL Header Encapsulation
WANG PC
Wang WITA
WANG WPS Comm.

Windows Animated Cursor Windows Bitmap	
Windows Ritman	
Williams Billiap	
Windows C++ Object Storage	
Windows Icon Cursor	
Windows Metafile	
Windows Micrografx Draw (DRW)	
Windows Palette	
Windows Media Video (WMV)	
Windows Media Audio (WMA)	
Windows Video (AVI)	
WinZip (unzip reader)	
WinZip	
Word Connection	
WordERA (V 1.0)	
WordMARC word processor	
WordPad	
WordPerfect General File	
WordPerfect Graphics 1	
WordPerfect Graphics 2	
WordStar	
WordStar 2000	
WordStar 6.0	
WriteNow	
Writing Assistant word processor	
X Bitmap (XBM)	

**Table 33-2** Formats supported for file type identification (continued)

Message Attachment or File Type Match formats	
X Image	
X Pixmap (XPM)	
Xerox 860 Comm.	
Xerox Writer word processor	
XHTML	
XML (generic)	
XML Paper Specification	
XyWrite	

## Supported formats for content extraction

Symantec Data Loss Prevention cracks more than 100 file formats for performing content extraction. You use content-based detection conditions to crack a file and extract its contents.

See "Content matching conditions" on page 301.

Table 33-3 lists the various file format categories whose content Symantec Data Loss Prevention can extract. Refer to the associated link for the individual file formats supported for that category.

See "Overview of detection file format support" on page 667.

**Table 33-3** Supported file format categories for content extraction

File format category	Default support list
Word-processing file formats	See "Supported word-processing formats for content extraction" on page 685.
Presentation file formats	See "Supported presentation formats for content extraction" on page 686.
Spreadsheet file formats	See "Supported spreadsheet formats for content extraction" on page 687.
Text and markup file formats	See "Supported text and markup formats for content extraction" on page 688.
Email file formats	See "Supported email formats for content extraction" on page 689.
CAD file formats	See "Supported CAD formats for content extraction" on page 690.

**Table 33-3** Supported file format categories for content extraction (continued)

File format category	Default support list
Graphics file formats	See "Supported graphics formats for content extraction" on page 690.
Database file formats	See "Supported database formats for content extraction" on page 690.
Other file formats	See "Other file formats supported for content extraction" on page 691.
Encapsulation file formats	See "Supported encapsulation formats for subfile extraction" on page 691.

#### Supported word-processing formats for content extraction

Table 33-4 lists the word-processing file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

Supported word-processing file formats for content extraction Table 33-4

Format Name	Format Extension
Adobe Maker Interchange Format (FrameMaker)	MIF
Apple iWork Pages	PAGES
ApplixWords	AW
Corel WordPerfect Linux	WPS
Corel WordPerfect Macintosh	WPS
Corel WordPerfect Windows	WO
Corel WordPerfect Windows	WPD
DisplayWrite	IP
Folio Flat file	FFF
Fujitsu Oasys	OA2
Haansoft Hangul	HWP
IBM DCA/RFT (Revisable Form Text)	DC
JustSystems Ichitaro	JTD
Lotus AMI Pro	SAM
Lotus AMI ProfessionalWrite Plus	AMI

Table 33-4 Supported word-processing file formats for content extraction (continued)

Format Name	Format Extension
LotusWord Pro	LWP
Lotus SmartMaster	MWP
Microsoft Word PC	DOC
Microsoft Word Windows	DOC
Microsoft Word Windows XML	DOCX
Microsoft Word Windows Template XML	DOTX
Microsoft Word Windows Macro-Enabled Template XML	DOTM
Microsoft Word Macintosh	DOC
Microsoft Works	WPS
Microsoft Windows Write	WRI
Microsoft OneNote	ONE
OpenOfficeWriter	SXW
OpenOfficeWriter	ODT
StarOfficeWriter	SXW
StarOfficeWriter	ODT
WordPad	RTF
XML Paper Specification	XPS
XyWrite	XY4

# Supported presentation formats for content extraction

Table 33-5 lists the presentation file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

Supported presentation formats for files content extraction Table 33-5

Format Name	Format Extension
Apple iWork Keynote	KEYNOTE

**Table 33-5** Supported presentation formats for files content extraction (continued)

Format Name	Format Extension
Applix Presents	AG
Corel Presentations	SHW
Lotus Freelance Graphics	PRZ
Lotus Freelance Graphics 2	PRE
Macromedia Flash	SWF
Microsoft PowerPoint Windows	PPT
Microsoft PowerPoint PC	PPT
Microsoft PowerPoint Windows XML	PPTX
Microsoft PowerPoint Windows Macro-Enabled XML	PPTM
Microsoft PowerPoint Windows XML Template	POTX
Microsoft PowerPoint Windows Macro-Enabled XML Template	РОТМ
Microsoft PowerPoint Windows XML Show	PPSX
Microsoft PowerPoint Windows Macro-Enabled Show	PPSM
Microsoft PowerPoint Macintosh	PPT
OpenOffice Impress	SXI
OpenOffice Impress	SXP
OpenOffice Impress	ODP
StarOffice Impress	SXI
StarOffice Impress	SXP
StarOffice Impress	ODP

# Supported spreadsheet formats for content extraction

Table 33-6 lists the spreadsheet file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

**Table 33-6** Supported spreadsheet formats for file contents extraction

Format Name	Format Extension
Apple iWork Numbers	NUMBERS
Applix Spreadsheets	AS
Comma Separated Values	CSV
Corel Quattro Pro	WB2
Corel Quattro Pro	WB3
Data Interchange Format	DIF
Lotus 1-2-3	123
Lotus 1-2-3	WK4
Lotus 1-2-3 Charts	123
Microsoft Excel Windows	XLS
Microsoft Excel Windows XML	XLSX
Microsoft Excel Charts	XLS
Microsoft Excel 2007 Binary	XLSB
Microsoft Excel Macintosh	XLS
Microsoft Works Spreadsheet	S30
Microsoft Works Spreadsheet	S40
OpenOffice Calc	SXC
OpenOffice Calc	ODS
StarOffice Calc	SXC
StarOffice Calc	ODS

# Supported text and markup formats for content extraction

Table 33-7 lists the text and markup file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

Supported text and markup file formats for content extraction **Table 33-7** 

Format Name	Format Extension
ANSI	TXT
ASCII	TXT
HTML	НТМ
Microsoft Excel Windows XML	XML
Microsoft Word Windows XML	XML
Microsoft Visio XML	VDX
Oasis Open Document Format	ODT
Oasis Open Document Format	ODS
Oasis Open Document Format	ODP
Rich Text Format	RTF
Unicode Text	TXT
XHTML	НТМ
XML (generic)	XML

## Supported email formats for content extraction

Table 33-8 lists the email file formats whose content Symantec Data Loss Prevention can extract for evaluation.

Supported email file formats for content extraction **Table 33-8** 

Format Name	Format Extension
Domino XML Language	DXL
EMC EmailXtender Native Message	ONM
Microsoft Outlook	MSG
Microsoft Outlook Express	EML
Text Mail (MIME)	various
Transfer Neutral Encapsulation Format	various

## Supported CAD formats for content extraction

Table 33-9 lists the computer-aided design (CAD) file formats whose content Symantec Data Loss Prevention can extract for evaluation.

**Table 33-9** Supported CAD file formats

Format Name	Format Extension
AutoCAD Drawing	DWG
AutoCAD Drawing Exchange	DFX
Microsoft Visio	VSD
Microstation	DGN

## Supported graphics formats for content extraction

Table 33-10 lists the graphics file formats whose content Symantec Data Loss Prevention can extract for evaluation.

Table 33-10 Supported graphics file formats for content extraction

Format Name	Format Extension
Enhanced Metafile	EMF
Lotus Pic	PIC
Tagged Image File (metadata only)	TIFF
Windows Metafile	WMF

#### Supported database formats for content extraction

The following table lists the database file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

Table 33-11 Crackable database file formats

Format Name	Format Extension
Microsoft Access	MDB
Microsoft Project	MPP

#### Other file formats supported for content extraction

Table 33-12 lists other file formats whose content Symantec Data Loss Prevention can extract for policy evaluation.

Table 33-12 Other supported formats for content extraction

Format Name	Format Extension
Adobe PDF	PDF
MPEG-1 Audio layer 3 (metadata only)	MP3
Microsoft Windows Backup Utility File	BKF
File Share Encryption (PGP Netshare)	You can decrypt Symantec File Share encrypted files and extract file contents for policy evaluation using the File Share plugin. Refer to the Symantec Data Loss Prevention Encryption Insight Implementation Guide.
	Note: Encryption Insight is only available with Network Discover.
Custom	You can write a plug-in to perform content, subfile, and metadata extraction operations on custom file formats. Refer to the Symantec Data Loss Prevention Content Extraction Plug-in Developers Guide.
	Note: Content extraction plug-ins are limited to detection servers.

# Supported encapsulation formats for subfile extraction

Symantec Data Loss Prevention supports various encapsulation formats for subfile extraction, such as ZIP, RAR, and TAR. The system automatically performs subfile extraction for supported formats using content-based match conditions. Subfile extraction is a subset of content extraction in that, if the system is successful in extracting a subfile from a supported encapsulated file, the system automatically extracts the text-based subfile contents if the subfile format is supported for content extraction.

See "Overview of detection file format support" on page 667.

Table 33-13 lists the file formats whose content Symantec Data Loss Prevention can extract for content evaluation.

Format Name	Format Extension
7-Zip	7Z
BinHex	HQX
GZIP	GZ
Java Archive	JAR
Microsoft Cabinet	CAB
Microsoft Compressed Folder	LZH
Microsoft Compressed Folder	LHA
PKZIP	ZIP
WinZip	ZIP
RAR archive	RAR
Tape Archive	TAR
UNIX Compress	Z
UUEncoding	UUE
YENC	YENC (server only)

Table 33-13 Supported encapsulation formats for subfile extraction

# Supported file formats for metadata extraction

Table 33-14 lists some of the file formats that Symantec Data Loss Prevention supports for metadata detection, and provides some example metadata fields returned for those formats.

This list is not exhaustive and is provided for quick reference only. Other file formats may be supported, and other custom fields may be returned. The best practice is to always use the filter utility to verify metadata support for each file format you want to detect.

See "Always use the filter utility to verify file format metadata support" on page 695.

File formats	Metadata	Description
Microsoft Office documents, for example:  Word (DOC, DOCX)  Excel (XLS, XLSX)  PowerPoint (PPT, PPTX)	For Microsoft Office documents, the system extracts Object Linking and Embedding (OLE) metadata.	Example fields:  Title Subject Author Keywords Other custom fields
Adobe PDF files	For Adobe PDF files, the system extracts Document Information Dictionary (DID) metadata. The system does not support Adobe Extensible Metadata Platform (XMP) metadata extraction.	Example fields:  Author Title Subject Creation Update dates
Other file formats (including binary and text)	Use the <i>filter</i> utility to verify metadata extraction for other file formats.	See "Always use the filter utility to verify file format metadata support" on page 695.
Custom file formats	Custom file type metadata	Content extraction plug-in that supports the metadata extraction operation.

Table 33-14 Supported file formats for metadata detection

#### About document metadata detection

In addition to file content and subfile extraction, Symantec Data Loss Prevention supports metadata extraction for many file formats. File format metadata is data about a file that is stored as file properties. By default metadata extraction is disabled because it can lead to false positives. Used properly, metadata detection can enhance the accuracy of your content-based policy rules.

For example, consider a business that uses Microsoft Office templates for their Word, Excel, and PowerPoint documents. The business applies Microsoft OLE metadata properties in the form of keywords to each template. The business has enabled metadata extraction and deployed keyword policies to match on metadata keywords. These policies can detect keywords in documents that are derived from the templates. The business also has the flexibility to use policy exceptions to avoid generating incidents if certain metadata keywords are present.

#### Enabling server metadata detection

By default metadata extraction is disabled for detection servers.

#### To enable server metadata extraction

- Log on to the Enforce Server administration console as a system administrator.
- Navigate to the System > Servers > Overview > Server Detail screen for the detection server you want to enable metadata extraction.
- 3 Click the **Server Settings** button.
- Locate property ContentExtraction. EnableMetaData in the list.
- 5 Enter the value **on** for this property to enable metadata extraction.
- 6 Click Save to save the configuration.
- 7 Click **Recycle the server** at the **Server Detail** screen to restart the server.
- Click **Done** at the **Server Detail** screen to complete the process.

#### Enabling endpoint metadata detection

By default metadata extraction is disabled for endpoints.

#### To enable endpoint metadata extraction

- Log on to the Enforce Server administration console as a system administrator.
- 2 Navigate to the **System > Agents > Agent Configuration** screen for the endpoint server you want to enable metadata extraction.
- Create a new endpoint configuration for metadata detection, or select the default configuration.
  - See "Create a separate endpoint configuration for metadata detection" on page 699.
- Select the **Advanced Agent Settings** tab.
- 5 Locate property Detection. ENABLE METADATA. str in the list.
- 6 Enter the value **on** for this property to enable metadata extraction.
- 7 Click **Save and Apply** to save the configuration change.

#### Best practices for using metadata detection

Best practices for using metadata detection lists best practices for implementing metadata detection with links to corresponding topics for detailed considerations.

Consideration	Торіс
Always use <i>filter</i> to verify file format metadata support.	See "Always use the filter utility to verify file format metadata support" on page 695.
Enable metadata detection only if it is necessary.	See "Distinguish metadata from file content and application data" on page 697.
Avoid generating false positives by selecting keywords carefully.	See "Use and tune keyword lists to avoid false positives on metadata" on page 699.
Understand resource implications of endpoint metadata extraction.	See "Understand performance implications of enabling endpoint metadata detection" on page 699.
Create a separate endpoint configuration for metadata detection.	See "Create a separate endpoint configuration for metadata detection" on page 699.
Use response rules to add metadata tags to incidents.	See "Use response rules to tag incidents with metadata" on page 699.

Table 33-15 Considerations for implementing metadata detection

#### Always use the filter utility to verify file format metadata support

To help you create policies that detect file format metadata, use the *filter* utility that is available with any Symantec Data Loss Prevention detection or Endpoint Server installation. This utility provides an easy way to determine which metadata fields the system returns for a given file format. The utility generates output that contains the metadata the system will extract at runtime for each file format you test using filter.

To verify file format metadata extraction support using filter describes how to use the filter utility. It is recommended that you always follow this process so that you can create and tune policies that accurately detect file format metadata.

Note: The data output by the *filter* utility is in ASCII format. Symantec Data Loss Prevention processes data in Unicode format. Therefore, you may rely on the existence of the fields returned by the filter utility, but the metadata detected by Symantec Data Loss Prevention may not look identical to the filter output.

#### To verify file format metadata extraction support using filter

- On the file system where a detection server is installed, start a command prompt session.
- 2 Change directory to where the filter utility is located.

For example, on a default 64-bit Windows installation you would issue the following command:

```
cd \SymantecDLP\Protect\plugins\contentextraction\Verity\x64
```

Issue the following command to run the filter program and display its syntax 3 and optional parameters.

```
filter -help
```

As indicated by the help, you use the following syntax to execute the *filter* utility:

```
filter [options] inputfile outputfile
```

The inputfile is an instance of the file format you want to verify. The outputfile is a file the filter utility writes the extracted data to.

Note the following extraction options:

- To verify metadata extraction, use the "get doc summary info" option:-i
- To verify content extraction, use no options: filter inputfile outputfile
- 4 Execute *filter* against an instance of the file format to verify metadata extraction.

For example, on Windows you would issue the following command:

```
filter -i \temp\myfile.doc \temp\metadata output.txt
```

Where myfile.doc is a file containing metadata you want to verify and have copied to the \temp directory, and metadata\_output.txt is the name of the file you want the system to generate and write the extracted data to.

5 Review the *filter* output. The output data should be similar to the following:

```
1 2 1252 CodePage 1 1 "S" Title 0 0 (null) 1 1 "P" Author 0 0 (null)
0 0 (null) 0 1 "" (null) 1 1 "m" LastAuthor 1 1 "1" RevNumber
1 3 6300 Minutes EditTime 1 3 Mon Aug 27 11:53:07 2007 LastPrinted
```

Refer to the following tables for an explanation of each metadata extraction 6 field output by the *filter* utility.

```
Table 33-16 repeats the output from Step 5, formatted for readability.
```

Table 33-17 explains each column field.

EditTime

LastPrinted

	•	•	
Column 1	Column 2	Column 3	Column 4
1	2	1252	CodePage
1	1	"S"	Title
0	0	(null)	
1	1	"P"	Author
0	0	(null)	
0	0	(null)	
0	1	···	(null)
1	1	"m"	LastAuthor
1	1	"1"	RevNumber

Table 33-16 Example filter metadata output

Table 33-17 Metadata fields generated by the filter utility

6300 Minutes

Mon Aug 27 11:53:07 2007

3

3

1

1

Column 1	Column 2	Column 3	Column 4
1 = valid field	The type of data:	The data payload for the	The name of the field (empty
0 = invalid field	1 = String	field.	or null if the field is invalid).
Note: You may ignore rows	2 = Integer		
where the first column is 0.	3 = Date/Time		
	5 = Boolean		

#### Distinguish metadata from file content and application data

Do not confuse metadata extraction with content extraction or application data. Some text that may appear to be metadata is extracted as content or application data. Table 33-18 describes some types of data that is not extracted as file format metadata to help you determine if and when you need to enable metadata detection.

Supported file formats for metadata extraction

Note: This list is not exhaustive and is provided for quick reference only. There may be other types of data that are not extracted as metadata. The best practice is to use the filter utility to verify file format metadata support. See "Always use the filter utility to verify file format metadata support" on page 695.

Data not extracted as metadata **Table 33-18** 

Content type	Extraction method
Application data	Application data including message transport information is extracted separately from file format extraction. For all inbound messages, the system extracts message envelope (header) and subject information as text at the application layer. The type of application data that is extracted depends on the channels supported by the detection server or endpoint.
Headers and footers	Document header and footer text is extracted as content, not metadata. To avoid false positives, it is recommended that you remove or whitelist headers and footers from documents.
	See "Use whitelisting to exclude non-sensitive content from partial matching" on page 503.
	See the Indexed Document Matching (IDM) chapter in the <i>Symantec Data Loss Prevention Administration Guide</i> for details.
Markup text	Markup text is extracted as content, not metadata. Markup text extraction is supported for HTML, XML, SGML, and more. Markup text extraction is disabled by default.
	See "Advanced server settings" on page 203.
	See "Advanced agent settings" on page 1414.
	See the "Advanced Server Settings" topic in the Symantec Data Loss Prevention Administration Guide to enable it.
Hidden text	Hidden text is extracted as content, not metadata. Hidden text extraction in the form of tracked changes is supported for some Microsoft Office file formats. Hidden text extraction is disabled by default.
	See "Advanced server settings" on page 203.
	See "Advanced agent settings" on page 1414.
	See the "Advanced Server Settings" topic in the Symantec Data Loss Prevention Administration Guide to enable it.
Watermarks	Text-based watermarks are extracted as content, not metadata. Text-based watermark detection is supported for Microsoft Word documents (versions 2003 and 2007). It is not supported for other file formats.

#### Use and tune keyword lists to avoid false positives on metadata

Enabling metadata extraction can cause false positives because more text is checked for a match. For example, if you have a policy that detects keywords and metadata extraction is enabled, the policy reports a match if a keyword is present in the content or in the metadata. Once the system has extracted the content and the metadata, the text is normalized and streamed to the detection component for matching. The detection component has no knowledge of the source of the text. whether it is application data, content, or metadata.

To detect file format metadata, you define keyword conditions for rules or exceptions that contain keywords that are specific to one or more file formats. To avoid generating false positives, clearly define the keyword lists in your policies. The keywords you use to detect metadata should be unique and distinct from keywords or phrases you use to detect content. Test and tune keyword lists to improve metadata detection accuracy.

#### Understand performance implications of enabling endpoint metadata detection

On the endpoint, enabling metadata extraction does not add overhead if no content rules are deployed. If content rules are deployed to the endpoint, enabling metadata extraction may introduce minor overhead because there is extra data to inspect. Test and tune your endpoint policy keyword lists to ensure that metadata detection is efficient.

#### Create a separate endpoint configuration for metadata detection

When you enable endpoint metadata detection, consider creating a custom endpoint configuration specifically for metadata detection. By doing so you can easily revert to the default configuration if necessary.

#### Use response rules to tag incidents with metadata

You cannot use metadata detection to apply tags to inbound files or documents that generate incidents. If this is desired, consider using a FlexResponse plug-in.

See "About response rules" on page 875.

See the Symantec Data Loss Prevention Administration Guide for details.

# Library of system data identifiers

This chapter includes the following topics:

- Libary of system data identifiers
- ABA Routing Number data identifier
- Australian Medicare Number data identifier
- Australian Tax File Number data identifier
- Burgerservicenummer data identifier
- Canadian Social Insurance Number data identifier
- Codice Fiscale data identifier
- Credit Card Magnetic Stripe Data data identifier
- Credit Card Number data identifier
- CUSIP Number data identifier
- Drivers License Number CA State data identifier
- Drivers License Number FL, MI, MN States data identifier
- Drivers License Number IL State data identifier
- Drivers License Number NJ State data identifier
- Drivers License Number NY State data identifier
- French INSEE Code data identifier

- Hong Kong ID data identifier
- IBAN Central data identifier
- IBAN East data identifier
- IBAN West data identifier
- IP Address data identifier
- National Drug Code (NDC) data identifier
- People's Republic of China ID data identifier
- Randomized US Social Security Number (SSN) data identifier
- Singapore NRIC data identifier
- South Korea Resident Registration Number data identifier
- Spanish DNI ID data identifier
- SWIFT Code data identifier
- Swiss AHV Number data identifier
- Taiwan ID data identifier
- UK Drivers License Number data identifier
- **UK Electoral Roll Number data identifier**
- UK National Health Service (NHS) Number data identifier
- **UK National Insurance Number data identifier**
- **UK Passport Number data identifier**
- UK Tax ID Number data identifier
- US Individual Tax Identification Number (ITIN) data identifier
- US Social Security Number (SSN) data identifier

# Libary of system data identifiers

This section lists all data identifiers provided by the Data Loss Prevention system.

# ABA Routing Number data identifier

The American Banking Association (ABA) routing number, also known as a routing transit number (RTN), is used to identify financial institutions and process transactions.

The ABA Routing Number data identifier detects 9-digit numbers and provides three breadths of detection:

The wide breadth edition validates the detected number using the final check digit.

See "ABA Routing Number wide breadth" on page 704.

The medium breadth edition validates the detected number using the final check digit and eliminates common test numbers.

See "ABA Routing Number medium breadth" on page 705.

The narrow breadth edition validates the detected number using the final check digit, eliminates common test numbers, and requires the presence of an ABA-related keyword.

See "ABA Routing Number narrow breadth" on page 705.

#### ABA Routing Number wide breadth

The wide breadth edition of the ABA Routing Number data identifier detects 9-digit numbers. It validates the number using the final check digit.

**Table 34-1** ABA Routing Number wide breadth patterns

Pattern		
[0123678]\d{8}		
[0123678]\d{3}-\d{4}-\d		

<b>Table 34-2</b> ABA Routing Number wide breadth va	aiidators
--	-----------

Mandatory validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted check sum.

#### ABA Routing Number medium breadth

The medium breadth edition of the ABA Routing number DI detects 9-digit numbers. It validates the number using the final check digit.

It eliminates common test numbers, such as 123456789, ranges reserved for future use, and all the same digit.

**Table 34-3** ABA Routing Number medium breadth patterns

Pattern	
[0123678]\d{8}	
[0123678]\d{3}-\d{4}-\d	

**Table 34-4** ABA Routing Number medium breadth validators

Mandatory validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted check sum.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.  Input: 123456789
Duplicate digits	Ensures that a string of digits are not all the same.
Number delimiter	Validates a match by checking the surrounding numbers.

## ABA Routing Number narrow breadth

The narrow breadth edition of the ABA Routing number data identifier detects 9-digit numbers and validates the number using the final check digit. It eliminates common test numbers, such as 123456789, ranges reserved for future use, and all the same digit. It also requires the presence of an ABA-related keyword.

**Table 34-5** ABA Routing Number narrow breadth patterns

Pattern	
[0123678]\d{8}	
[0123678]\d{3}-\d{4}-\d	

**Table 34-6** ABA Routing Number narrow breadth validators

Mandatory validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted checksum.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.  Input: 123456789
Duplicate digits	Ensures that a string of digits are not all the same.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched. Input:  aba, aba #, aba routing #, aba routing number, aba#, abarouting#, abaroutingnumber, american bank association routing #, american bank association routing number, americanbankassociationrouting#, americanbankassociationroutingmumber, bank routing #, bank routing number, bankroutingnumber
Number delimiter	Validates a match by checking the surrounding numbers.

## ABA Routing Number wide breadth

The wide breadth edition of the ABA Routing Number data identifier detects 9-digit numbers. It validates the number using the final check digit.

**Table 34-7** ABA Routing Number wide breadth patterns

Pattern				
[0123678]\d{8}				
[0123678]\d{3}-\d{4}-\d				
Table 34-8 ABA Routing Number wide breadth validators				
Mandatory validator	Description			
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted check sum.			

#### ABA Routing Number medium breadth

The medium breadth edition of the ABA Routing number DI detects 9-digit numbers. It validates the number using the final check digit.

It eliminates common test numbers, such as 123456789, ranges reserved for future use, and all the same digit.

**Table 34-9** ABA Routing Number medium breadth patterns

Pattern	
[0123678]\d{8}	
[0123678]\d{3}-\d{4}-\d	

Table 34-10 ABA Routing Number medium breadth validators

Mandatory validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted check sum.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.  Input: 123456789
Duplicate digits	Ensures that a string of digits are not all the same.
Number delimiter	Validates a match by checking the surrounding numbers.

#### ABA Routing Number narrow breadth

The narrow breadth edition of the ABA Routing number data identifier detects 9-digit numbers and validates the number using the final check digit. It eliminates common test numbers, such as 123456789, ranges reserved for future use, and all the same digit. It also requires the presence of an ABA-related keyword.

Table 34-11 ABA Routing Number narrow breadth patterns

Pattern			
[0123678]\d{8}			
[0123678]\d{3}-\d{4}-\d			

	Table 54-12	/ID// Nouting	G Number harrow breadth validators
ator			Description

ARA Routing Number narrow breadth validators

Tahla 3/1-12

Mandatory validator	Description
ABA Checksum	Every ABA routing number must start with the following two digits: 00-15,21-32,61-72,80 and pass an ABA specific, position-weighted checksum.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.  Input: 123456789
Duplicate digits	Ensures that a string of digits are not all the same.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched. Input:  aba, aba #, aba routing #, aba routing number, aba#, abarouting#, abaroutingnumber, american bank association routing #, american bank association routing number, americanbankassociationrouting#, americanbankassociationroutingnumber, bank routing #, bank routing number, bankroutingnumber
Number delimiter	Validates a match by checking the surrounding numbers.

# Australian Medicare Number data identifier

The Australian Medicare Number is a personal identifier allocated by the Australian Health Insurance Commission to eligible persons under the Medicare scheme. This number appears on the Australian Medicare card.

The Australian Medicare Number data identifier detects an 8- or 9-digit number that matches the format of the Australian Medicare Number. This data identifier does not implement any validators.

Australian Medicare Number wide breadth patterns Table 34-13

Pattern
\d{4} \d{5} \d \d
\d{4}-\d{5}-\d-\d

#### Australian Tax File Number data identifier

The Australian Tax File Number (TFN) is an 8- or 9-digit number issued by the Australian Taxation Office (ATO) to taxpayers (individual, company, superannuation fund, partnership or trust) to identify their Australian tax dealings.

The Australian Tax File Number data identifier detects an 8- or 9-digit number and ensures that the detected number passes checksum validation.

Table 34-14 Australian Tax File Number wide breadth patterns

Pattern		
\d{8}		
\d{9}		
Table 34-15Australian T	ax File Number wide breadth validator	
Mandatory validator	Description	
Australian Tax File validation check	Computes the checksum and validates the pattern against it.	

# Burgerservicenummer data identifier

In the Netherlands, the burgerservicenummer is used to uniquely identify citizens and is printed on driving licenses, passports and international ID cards under the header Personal Number.

The Burgerservicenummer data identifier detects an 8- or 9-digit number that passes checksum validation.

Table 34-16 Burgerservicenummer wide breadth pattern

Pattern		
\d{9}		
Table 34-17	Burgerservicenummer wide breadth validator	
Mandatory validator	Description	
Burgerservicenummer Check	Burgerservicenummer Check.	

## Canadian Social Insurance Number data identifier

The Canadian Social Insurance Number (SIN) is a personal identification number issued by Human Resources and Skills Development Canada primarily for administering national pension and employment plans.

The Canadian Social Insurance Number data identifier provides three breadths of detection:

- Wide See "Canadian Social Insurance Number wide breadth" on page 710.
- Medium See "Canadian Social Insurance Number medium breadth" on page 711.
- Narrow See "Canadian Social Insurance Number narrow breadth" on page 711.

#### Canadian Social Insurance Number wide breadth

The wide breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes, spaces, periods, slashes, or without separators. Performs Luhn check validation.

Table 34-18 Canadian Social Insurance Number wide breadth patterns

Pattern	
d{3} \d{3} \d{3}	
d{9}	
d{3}/\d{3}\/d{3}	
d{3}.\d{3}.\d{3}	
d{3}-\d{3}-\d{3}	

Table 34-19 Canadian Social Insurance Number wide breadth validator

Mandatory validator	Description
	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.

#### Canadian Social Insurance Number medium breadth

The medium breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes, spaces, or periods. It performs Luhn check validation and eliminates non-assigned numbers and common test numbers.

Canadian Social Insurance Number medium breadth patterns Table 34-20

Pattern			
\d{3} \d{3} \d{3}			
\d{3}.\d{3}.\d{3}			
\d{3}-\d{3}-\d{3}			

Canadian Social Insurance Number medium breadth validators Table 34-21

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.
Number delimiter	Validates a match by checking the surrounding numbers.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.
	Input:
	8, 123456789

#### Canadian Social Insurance Number narrow breadth

The narrow breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes or spaces. Performs Luhn check validation. Eliminates non-assigned numbers, fictitiously assigned numbers, and common test numbers. Requires the presence of a Social Insurance-related keyword.

Table 34-22 Canadian Social Insurance Number narrow breadth patterns

Pattern			
\d{3} \d{3} \d{3}			
\d{3}-\d{3}-\d{3}			

Table 34-23	Canadian So	cial Insurance Numbe	r narrow breadth validators
Table 34-23	Canadian 50	CIAL HISHIAHCE MUHIDE	er Harrow Dreauth Valluators

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.
Number delimiter	Validates a match by checking the surrounding numbers.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.
	Input:
	0, 8, 123456789
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
	Inputs:
	pension, pensions, soc ins, ins #, social ins, CSIN, SSN, social security, social insurance, Canada, Canadian

## Canadian Social Insurance Number wide breadth

The wide breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes, spaces, periods, slashes, or without separators. Performs Luhn check validation.

Table 34-24 Canadian Social Insurance Number wide breadth patterns

Pattern
\d{3} \d{3} \d{3}
\d{9}
\d{3}\\d{3}\\d{3}
\d{3}.\d{3}.\d{3}
\d{3}-\d{3}-\d{3}

Canadian Social Insurance Number wide breadth validator **Table 34-25** 

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.

#### Canadian Social Insurance Number medium breadth

The medium breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes, spaces, or periods. It performs Luhn check validation and eliminates non-assigned numbers and common test numbers.

Canadian Social Insurance Number medium breadth patterns Table 34-26

Pattern			
\d{3} \d{3} \d{3}			
\d{3}.\d{3}.\d{3}			
\d{3}-\d{3}-\d{3}			

Canadian Social Insurance Number medium breadth validators Table 34-27

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.
Number delimiter	Validates a match by checking the surrounding numbers.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.
	Input:
	8, 123456789

#### Canadian Social Insurance Number narrow breadth

The narrow breadth Canadian Social Insurance Number DI detects 9-digit numbers with the format DDD-DDD separated by dashes or spaces. Performs Luhn check validation. Eliminates non-assigned numbers, fictitiously assigned numbers, and common test numbers. Requires the presence of a Social Insurance-related keyword.

Table 34-28 Canadian Social Insurance Number narrow breadth patterns

Pattern	
\d{3} \d{3} \d{3}	
\d{3}-\d{3}-\d{3}	

Table 34-29 Canadian Social Insurance Number narrow breadth validators

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Canadian Insurance Number must pass.
Number delimiter	Validates a match by checking the surrounding numbers.
Exclude beginning characters	With this option selected, data beginning with any of the following list of values will not be matched.
	Input:
	0, 8, 123456789
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
	Inputs:
	pension, pensions, soc ins, ins #, social ins, CSIN, SSN, social security, social insurance, Canada, Canadian

# Codice Fiscale data identifier

In Italy the codice fiscale is issued to every Italian at birth. The codice fiscale uniquely identifies an Italian citizen or permanent resident alien and issuance of the code is centralized to the Ministry of Treasure.

The Codice Fiscale data identifier detects a 16 character identifier. The final character must match a checksum algorithm.

Table 34-30 Codice Fiscale wide breadth patterns

Pattern
[A-Z]{6}[0-9LMNPQRSTUV]{2}[ABCDEHLMPRST][0-9LMNPQRSTUV]{2}[A-Z] [0-9LMNPQRSTUV]{3}[A-Z]
$[A-Z]\{3\}\ [A-Z]\{3\}\ [0-9LMNPQRSTUV]\{2\}[ABCDEHLMPRST][0-9LMNPQRSTUV]\{2\}\ [A-Z][0-9LMNPQRSTUV]\{3\}[A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][3][A-Z][0-9LMNPQRSTUV][4][A-Z][0-9LMNPQRSTUV][4][A-Z][0-9LMNPQRSTUV][4][A-Z][A-Z][4][A-Z][4][A-Z][4][A-Z][4][A-Z][4][4][A-Z][4][4][A-Z][4][4][4][4][4][4][4][4][4][4][4][4][4]$
Table 34-31 Codice Fiscale wide breadth validator

Mandatory validator	Description
Codice Fiscale Control Key Check	Computes the control key and checks if it is valid.

# Credit Card Magnetic Stripe Data data identifier

The magnetic stripe of a credit card contains information about the card. Storage of the complete version of this data is a violation of the Payment Card Industry (PCI) Data Security Standard.

The Credit Card Magnetic Stripe Data data identifier detects the following raw data taken from the credit card magnetic stripe:

- Data from track 1, format B, which typically contains account number, name, expiration date, and possibly Card Verification Value or Card Verification Code 1 (CVV1/CVC1).
- Data from track 2, which typically contains account number and possibly expiration date, service code and Card Verification Value or Card Verification Code 1 (CVV1/CVC1)

The Credit Card Magnetic Stripe data identifier detects the characteristic data pattern for track 2 data which contains the start sentinel, format code, primary account number, name, expiration date, service code, discretional data, and the end sentinel. It also includes standard field separators. It validates the data using a Luhn check validator.

Credit Card Magnetic Stripe Data medium breadth patterns Table 34-32

- ·	Table 34-32 Credit Card Wagnetic Stripe Data Medium Dreadth patterns	
Pattern	Pattern (continued)	
;1800\d{11}=	%B3[068]\d{12}^[A-Z]{1}	
;6011-\d{4}-\d{4}-\d{4}=	%B3[068]\d{2} \d{6} \d{4}^[A-Z]{1}	
;6011 \d{4} \d{4} \d{4}=	%B3[068]\d{2}-\d{6}-\d{4}^[A-Z]{1}	
;6011\d{12}=	%B4\d{12}^[A-Z]{1}	
;3[068]\d{12}=	%B3[47]\d{2}-\d{6}-\d{5}^[A-Z]{1}	
;3[068]\d{2} \d{6} \d{4}=	%B4\d{3} \d{4} \d{4} \d{4}^[A-Z]{1}	
;3[068]\d{2}-\d{6}-\d{4}=	%B3[47]\d{2} \d{6} \d{5}^[A-Z]{1}	
;4\d{12}=	%B4\d{15}^[A-Z]{1}	
;3[47]\d{2}-\d{6}-\d{5}=	%B3[47]\d{13}^[A-Z]{1}	
;4\d{3} \d{4} \d{4} \d{4}=	%B5[1-5]\d{2}-\d{4}-\d{4}^(A-Z]{1}	
;3[47]\d{2} \d{6} \d{5}=	%B4\d{3}-\d{4}-\d{4}-\d{4}^[A-Z]{1}	
;4\d{15}= ;3[47]\d{13}=	%B5[1-5]\d{2} \d{4} \d{4} \d{4}^[A-Z]{1}	
;5[1-5]\d{2}-\d{4}-\d{4}-\d{4}=	%B5[1-5]\d{14}^[A-Z]{1}	
;4\d{3}-\d{4}-\d{4}=	%B2131\d{11}^[A-Z]{1}	
;5[1-5]\d{2} \d{4} \d{4} \d{4}=	%B3\d{3}-\d{4}-\d{4}-\d{4}^[A-Z]{1}	
;5[1-5]\d{14}= ;2131\d{11}=	%B3\d{3} \d{4} \d{4} \d{4}^[A-Z]{1}	
;3\d{3}-\d{4}-\d{4}-\d{4}=	%B3\d{15}^[A-Z]{1}	
$3\d{3} \d{4} \d{4} \d{4} =$	%B2149\d{11}^[A-Z]{1}	
;3\d{15}=	%B2149 \d{6} \d{5}^[A-Z]{1}	
;2149\d{11}=	%B2149-\d{6}-\d{5}^[A-Z]{1}	
;2149 \d{6} \d{5}=	%B2014\d{11}^[A-Z]{1}	
;2149-\d{6}-\d{5}=	%B2014 \d{6} \d{5}^[A-Z]{1}	
;2014\d{11}=	%B2014-\d{6}-\d{5}^[A-Z]{1}	
;2014 \d{6} \d{5}=		
;2014-\d{6}-\d{5}=		
%B1800\d{11}^[A-Z]{1}		
%B6011-\d{4}-\d{4}-\d{4}^[A-Z]{1}		
%B6011 \d{4} \d{4} \d{4}^[A-Z]{1}		
%B6011\d{12}^[A-Z]{1}		

Table 34-33 Credit Card Magnetic Stripe Data medium breadth validator

Validator	Description
Luhn Check	Computes the Luhn checksum which every instance must pass.

#### Credit Card Number data identifier

Account number needed to process credit card transactions. Often abbreviated as CCN. Also known as a Primary Account Number (PAN).

The Credit Card Number data identifier offers three breadths of detection:

- Wide breadth See "Credit Card Number wide breadth" on page 720.
- Medium breadth See "Credit Card Number medium breadth" on page 721.
- Narrow breadth See "Credit Card Number narrow breadth" on page 723.

#### Credit Card Number wide breadth

The wide breadth Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators.

This validator includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa.

This validator performs Luhn check validation.

Table 34-34	Credit Card Number wide breadth patterr	S

Pattern	Pattern (continued)
\d{16}	2149-\d{6}-\d{5}
\d{4}.\d{4}.\d{4}	3[068]\d{12}
\d{4} \d{4} \d{4} \d{4}	3[068]\d{2}.\d{6}.\d{4}
\d{4}-\d{4}-\d{4}	3[068]\d{2} \d{6} \d{4}
1800\d{11} 2014.\d{6}.\d{5}	3[068]\d{2}-\d{6}-\d{4}
2014\d{11} 2014 \d{6} \d{5}	3[47]\d{13}
2014-\d{6}-\d{5}	3[47]\d{2}.\d{6}.\d{5}
2131\d{11}	3[47]\d{2} \d{6} \d{5}
2149.\d{6}.\d{5}	3[47]\d{2}-\d{6}-\d{5}
2149\d{11}	4\d{12}
2149 \d{6} \d{5}	

Table 34-35 Credit Card Number wide breadth validator

Mandatory validator	Description
Luhn Check	Computes the Luhn checksum which every Credit Card Number must pass.

#### Credit Card Number medium breadth

The medium breadth Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. This validator performs Luhn check validation. This validator includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa. This validator eliminates common test numbers, including those reserved for testing by credit card issuers.

Credit Card Number medium breadth patterns **Table 34-36** 

Pattern	Pattern (continued)
1800\d{11}	3\d{3}.\d{4}.\d{4}.\d{4}
2014.\d{6}.\d{5}	3\d{3} \d{4} \d{4} \d{4}
2014\d{11}	3\d{3}-\d{4}-\d{4}-\d{4}
2014 \d{6} \d{5}	4\d{12} 4\d{15}
2014-\d{6}-\d{5}	4\d{3}.\d{4}.\d{4}
2131\d{11}	4\d{3} \d{4} \d{4} \d{4}
2149.\d{6}.\d{5} 2149\d{11}	4\d{3}-\d{4}-\d{4}-\d{4}
2149 \d{6} \d{5}	5[1-5]\d{14}
2149-\d{6}-\d{5}	5[1-5]\d{2}.\d{4}.\d{4}
3[068]\d{12}	5[1-5]\d{2} \d{4} \d{4} \d{4}
3[068]\d{2}.\d{6}.\d{4}	5[1-5]\d{2}-\d{4}-\d{4}
3[068]\d{2} \d{6} \d{4}	6011.\d{4}.\d{4}.\d{4}
3[068]\d{2}-\d{6}-\d{4}	6011\d{12}
3[47]\d{13}	6011 \d{4} \d{4} \d{4}
3[47]\d{2}.\d{6}.\d{5}	6011-\d{4}-\d{4}-\d{4}
3[47]\d{2} \d{6} \d{5}	
3[47]\d{2}-\d{6}-\d{5}	
3\d{15}	

Credit Card Number medium breadth validators **Table 34-37** 

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Credit Card Number must pass.
Exclude data match	Excludes anything that matches the specified text.

**Table 34-37** Credit Card Number medium breadth validators (continued)

Mandatory validator	Description
Exclude data match inputs	011111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 30000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 340000000000009, 341019464477148, 34111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 4007000000027, 4012888888881880, 4024007116284, 41111111111111, 41111111111111, 42222222222
Number Delimiter	Validates a match by checking the surrounding number.

#### Credit Card Number narrow breadth

The narrow breadth edition of the Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. It performs Luhn check validation. Includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa. Eliminates common test numbers, including those reserved for testing by credit card issuers. Also requires presence of a credit card-related keyword.

Table 34-38 Credit Card Number narrow breadth patterns

Pattern	Pattern (continued)
2149 \d{6} \d{5}	5[1-5]\d{2}-\d{4}-\d{4}
2149-\d{6}-\d{5}	5[1-5]\d{2} \d{4} \d{4} \d{4}
2014\d{11}	5[1-5]\d{14}
2014 \d{6} \d{5}	5[1-5]\d{2}.\d{4}.\d{4}.\d{4}
2014-\d{6}-\d{5}	2131\d{11}
6011-\d{4}-\d{4}-\d{4}	3\d{3}-\d{4}-\d{4}-\d{4}
6011 \d{4} \d{4} \d{4}	3\d{3} \d{4} \d{4} \d{4}
6011\d{12}	3\d{15}
3[068]\d{12}	2149\d{11}
3[068]\d{2} \d{6} \d{4}	
3[068]\d{2}-\d{6}-\d{4}	
3[47]\d{2}-\d{6}-\d{5}	
3[47]\d{2} \d{6} \d{5}	
3[47]\d{13}	
4\d{3}-\d{4}-\d{4}-\d{4}	
3\d{3}.\d{4}.\d{4}.\d{4}	
2149.\d{6}.\d{5}	
2014.\d{6}.\d{5}	
6011.\d{4}.\d{4}.\d{4}	
3[068]\d{2}.\d{6}.\d{4}	
3[47]\d{2}.\d{6}.\d{5}	
4\d{3}.\d{4}.\d{4}.\d{4}	
1800\d{11}	
4\d{12}	
4\d{3} \d{4} \d{4} \d{4}	
4\d{15}	

Table 34-39 Credit Card Number narrow breadth validators

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Credit Card Number must pass.
Exclude data match	Excludes anything that matches the specified text.
Exclude data match inputs	011111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 3000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 308800000000000, 308800000000009, 3088272824427380, 3096666928988980, 3158060990195830, 34000000000009, 341019464477148, 3411111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 4007000000027, 4012888888881880, 4024007116284, 41111111111111, 4111111111111, 42222222222
Number Delimiter	Validates a match by checking the surrounding number.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords inputs	account number, account ps, american express, americanexpress, amex, bank card, bankcard, card num, card number, cc #, cc#, ccn, check card, checkcard, credit card, credit card #, credit card number, credit card#, debit card, debitcard, diners club, dinersclub, discover, enroute, japanese card bureau, jcb, mastercard, mc, visa

#### Credit Card Number wide breadth

The wide breadth Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. This validator includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa.

This validator performs Luhn check validation.

Credit Card Number wide breadth patterns Table 34-40

Pattern	Pattern (continued)
\d{16}	2149-\d{6}-\d{5}
\d{4}.\d{4}.\d{4}.\d{4}	3[068]\d{12}
\d{4} \d{4} \d{4} \d{4}	3[068]\d{2}.\d{6}.\d{4}
\d{4}-\d{4}-\d{4}	3[068]\d{2} \d{6} \d{4}
1800\d{11} 2014.\d{6}.\d{5}	3[068]\d{2}-\d{6}-\d{4}
2014\d{11} 2014 \d{6} \d{5}	3[47]\d{13}
2014-\d{6}-\d{5}	3[47]\d{2}.\d{6}.\d{5}
2131\d{11}	3[47]\d{2} \d{6} \d{5}
2149.\d{6}.\d{5}	3[47]\d{2}-\d{6}-\d{5}
2149\d{11}	4\d{12}
2149 \d{6} \d{5}	

Credit Card Number wide breadth validator Table 34-41

Mandatory validator	Description
Luhn Check	Computes the Luhn checksum which every Credit Card Number must pass.

# Credit Card Number medium breadth

The medium breadth Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. This validator performs Luhn check validation. This validator includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa. This validator eliminates common test numbers, including those reserved for testing by credit card issuers.

Table 34-42 Credit Card Number medium breadth patterns

Pattern	Pattern (continued)
1800\d{11}	3\d{3}.\d{4}.\d{4}.\d{4}
2014.\d{6}.\d{5}	3\d{3} \d{4} \d{4} \d{4}
2014\d{11}	3\d{3}-\d{4}-\d{4}-\d{4}
2014 \d{6} \d{5}	4\d{12} 4\d{15}
2014-\d{6}-\d{5}	4\d{3}.\d{4}.\d{4}
2131\d{11}	4\d{3} \d{4} \d{4} \d{4}
2149.\d{6}.\d{5} 2149\d{11}	4\d{3}-\d{4}-\d{4}-\d{4}
2149 \d{6} \d{5}	5[1-5]\d{14}
2149-\d{6}-\d{5}	5[1-5]\d{2}.\d{4}.\d{4}
3[068]\d{12}	5[1-5]\d{2} \d{4} \d{4} \d{4}
3[068]\d{2}.\d{6}.\d{4}	5[1-5]\d{2}-\d{4}-\d{4}-\d{4}
3[068]\d{2} \d{6} \d{4}	6011.\d{4}.\d{4}.\d{4}
3[068]\d{2}-\d{6}-\d{4}	6011\d{12}
3[47]\d{13}	6011 \d{4} \d{4} \d{4}
3[47]\d{2}.\d{6}.\d{5}	6011-\d{4}-\d{4}-\d{4}
3[47]\d{2} \d{6} \d{5}	
3[47]\d{2}-\d{6}-\d{5}	
3\d{15}	

Credit Card Number medium breadth validators **Table 34-43** 

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Credit Card Number must pass.
Exclude data match	Excludes anything that matches the specified text.

**Table 34-43** Credit Card Number medium breadth validators (continued)

Mandatory validator	Description
Exclude data match inputs	011111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 30000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 34000000000000, 341019464477148, 34111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 40070000000027, 4012888888881880, 4024007116284, 41111111111111, 4111111111111, 42222222222
Number Delimiter	Validates a match by checking the surrounding number.

### Credit Card Number narrow breadth

The narrow breadth edition of the Credit Card Number data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. It performs Luhn check validation. Includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa. Eliminates common test numbers, including those reserved for testing by credit card issuers. Also requires presence of a credit card-related keyword.

Table 34-44 Credit Card Number narrow breadth patterns

Pattern	Pattern (continued)
2149 \d{6} \d{5}	5[1-5]\d{2}-\d{4}-\d{4}-\d{4}
2149-\d{6}-\d{5}	5[1-5]\d{2} \d{4} \d{4} \d{4}
2014\d{11}	5[1-5]\d{14}
2014 \d{6} \d{5}	5[1-5]\d{2}.\d{4}.\d{4}.\d{4}
2014-\d{6}-\d{5}	2131\d{11}
6011-\d{4}-\d{4}-\d{4}	3\d{3}-\d{4}-\d{4}-\d{4}
6011 \d{4} \d{4} \d{4}	3\d{3} \d{4} \d{4} \d{4}
6011\d{12}	3\d{15}
3[068]\d{12}	2149\d{11}
3[068]\d{2} \d{6} \d{4}	
3[068]\d{2}-\d{6}-\d{4}	
3[47]\d{2}-\d{6}-\d{5}	
3[47]\d{2} \d{6} \d{5}	
3[47]\d{13}	
4\d{3}-\d{4}-\d{4}	
3\d{3}.\d{4}.\d{4}.\d{4}	
2149.\d{6}.\d{5}	
2014.\d{6}.\d{5}	
6011.\d{4}.\d{4}.\d{4}	
3[068]\d{2}.\d{6}.\d{4}	
3[47]\d{2}.\d{6}.\d{5}	
4\d{3}.\d{4}.\d{4}.\d{4}	
1800\d{11}	
4\d{12}	
4\d{3} \d{4} \d{4} \d{4}	
4\d{15}	

Table 34-45 Credit Card Number narrow breadth validators

Mandatory validator	Description
Luhn Check	Validator computes the Luhn checksum which every Credit Card Number must pass.
Exclude data match	Excludes anything that matches the specified text.
Exclude data match inputs	0111111111111111, 1234567812345670, 180025848680889, 180026939516875, 20140000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 3000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 308800000000000, 308800000000009, 3088272824427380, 3096666928988980, 3158060990195830, 34000000000000, 341019464477148, 3411111111111, 341132368578216, 343510064010360, 344400377306201, 353011133330000, 3566002020360500, 37000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 40070000000027, 4012888888881880, 4024007116284, 41111111111111, 4111111111111, 42222222222
Number Delimiter	Validates a match by checking the surrounding number.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords inputs	account number, account ps, american express, americanexpress, amex, bank card, bankcard, card num, card number, cc #, cc#, ccn, check card, checkcard, credit card, credit card #, credit card number, credit card#, debit card, debitcard, diners club, dinersclub, discover, enroute, japanese card bureau, jcb, mastercard, mc, visa

### CUSIP Number data identifier

The CUSIP number is a unique identifier assigned to North American stock or other securities. This number is issued by the Committee on Uniform Security Identification Procedures (CUSIP) to assist in clearing and settling trades.

The CUSIP Number data identifier detects 9 character strings.

This data identifier provides three breadths of detection:

- The wide edition validates the final check digit. See "CUSIP Number wide breadth" on page 728.
- The medium edition validates the final check digit and requires the presence of a keyword.

See "CUSIP Number medium breadth" on page 728.

The narrow edition validates the final check digit and requires the presence of a keyword.

See "CUSIP Number narrow breadth" on page 729.

#### CUSIP Number wide breadth

The wide breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits. Validates the final check digit.

Table 34-46 CUSIP Number wide breadth pattern

Pattern			
\d{4}\w{4}\d			

Table 34-47	CUSIP	Number	wide	breadth	validator
-------------	-------	--------	------	---------	-----------

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).

#### CUSIP Number medium breadth

The medium breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits.

This edition of the validator validates the final check digit and also requires the presence of a CUSIP-related keyword..

Table 34-48 CUSIP Number medium breadth pattern

Pattern			
\d{4}\w{4}\d			

CUSIP Number medium breadth validator Table 34-49

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, NNA, National Securities Identification Number

#### CUSIP Number narrow breadth

The narrow breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits.

This edition of the validator validates the final check digit and also requires the presence of a CUSIP-related keyword.

This edition of the data identifier is narrower than the medium breadth because it does not include the "NNA" abbreviation as a keyword.

Table 34-50 CUSIP Number narrow breadth pattern

Pattern	
\d{4}\w{4}\d	

Table 34-51 CUSIP Number narrow breadth validators

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.

Table 34-51 CUSIP Number narrow breadth validators (continued)

Mandatory validator	Description
Find keywords input	cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, National Securities Identification Number

#### CUSIP Number wide breadth

The wide breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits. Validates the final check digit.

Table 34-52 CUSIP Number wide breadth pattern

Pattern			
\d{4}\w{4}\d			

#### CUSIP Number wide breadth validator Table 34-53

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).

# **CUSIP** Number medium breadth

The medium breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits.

This edition of the validator validates the final check digit and also requires the presence of a CUSIP-related keyword..

Table 34-54 CUSIP Number medium breadth pattern

Pattern	
\d{4}\w{4}\d	

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, NNA, National Securities Identification Number

**Table 34-55** CUSIP Number medium breadth validator

# CUSIP Number narrow breadth

The narrow breadth edition of the CUSIP Number data identifier detects 9 character strings. The 5th, 6th, 7th, and 8th character can be a letter or number, and all others are digits.

This edition of the validator validates the final check digit and also requires the presence of a CUSIP-related keyword.

This edition of the data identifier is narrower than the medium breadth because it does not include the "NNA" abbreviation as a keyword.

Table 34-56 CUSIP Number narrow breadth pattern

Pattern	
\d{4}\w{4}\d	

CUSIP Number narrow breadth validators Table 34-57

Mandatory validator	Description
Cusip Validation	Validator checks for invalid CUSIP ranges and computes the CUSIP checksum (Modulus 10 Double Add Double algorithm).
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, National Securities Identification Number

### Drivers License Number – CA State data identifier

This number is the identification number for an individual's driver's license issued by the US state of California.

The Drivers License Number – CA State data identifier detects the presence of a 7-digit number.

This data identifier provides two breadths of validation:

- The wide breadth edition detects any 7-digit number. See "Drivers License Number – CA State wide breadth" on page 731.
- The medium breadth edition validates a detected number against keywords. See "Drivers License Number – CA State medium breadth" on page 731.

### Drivers License Number - CA State wide breadth

The wide breadth edition of the CA Driver License Number data identifier detects an 8 character string, beginning with a letter followed by a 7-digit number.

**Note:** This breadth option does not include any validators.

**Table 34-58** Drivers License Number wide breadth pattern

#### Pattern

 $Id{7}$ 

### Drivers License Number - CA State medium breadth

The medium breadth edition of this data identifier detects an 8 character string, beginning with a letter followed by a 7-digit number.

It validates a detected number by requiring a driver's license keyword AND a California-related keyword.

Drivers License Number – CA State medium breadth pattern Table 34-59

#### Pattern

 $Id{7}$ 

Table 34-60 Drivers License Number – CA State medium breadth validators

Mandatory validator	Description
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	ca, calif, california

#### Drivers License Number – CA State wide breadth

The wide breadth edition of the CA Driver License Number data identifier detects an 8 character string, beginning with a letter followed by a 7-digit number.

Note: This breadth option does not include any validators.

Drivers License Number wide breadth pattern Table 34-61

#### Pattern

 $Id{7}$ 

# Drivers License Number - CA State medium breadth

The medium breadth edition of this data identifier detects an 8 character string, beginning with a letter followed by a 7-digit number.

It validates a detected number by requiring a driver's license keyword AND a California-related keyword.

Table 34-62 Drivers License Number – CA State medium breadth pattern

#### Pattern

 $Id{7}$ 

Mandatory validator	Description
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	ca, calif, california

Drivers License Number – CA State medium breadth validators **Table 34-63** 

# Drivers License Number - FL, MI, MN States data identifier

These number are the identification number for an individual's driver's license issued by one of the following US states: Florida, Michigan, or Minnesota. These states are grouped together because they share a common pattern for this number.

This data identifier detects a 13 character string, beginning with a letter followed by 12 numbers.

This data identifier provides two breadths of validation:

- The wide breadth edition detects any 13 character string with a letter followed by 12 numbers.
  - See "Drivers License Number- FL, MI, MN States wide breadth" on page 734.
- The medium breadth narrows the scope by requiring the presence keywords. See "Drivers License Number-FL, MI, MN States medium breadth" on page 734.

# Drivers License Number- FL, MI, MN States wide breadth

The wide breadth edition of this data identifier detects any 13 character string with a letter followed by 12 numbers.

For the MN license number, the following format is matched: L-DDD-DDD-DDD-DDD.

Note: This breadth option does not include any validators.

**Table 34-64** 

Drivers License Number- FL, MI, MN States wide breadth patterns

#### **Patterns**

\\I \\d{3} \\d{3} \\d{3} \\d{3}

 $\ln \{12\}$ 

 $1/d{3}-d{3}-d{2}-d{3}-d$ 

 $I-d{3}-d{3}-d{3}$ 

# Drivers License Number- FL, MI, MN States medium breadth

The medium breadth edition of this data identifier implements patters to detect any 13 character string with a letter followed by 12 numbers. For the MN license number, the following format is matched: L-DDD-DDD-DDD-DDD.

This data identifier validates the number by requiring the presence of a drivers license keyword AND a state-related keyword.

**Table 34-65** Drivers License Number-FL, MI, MN States medium breadth patterns

Pattern
\\\ \\d{3} \\d{3} \\d{3} \\d{3}
\\\d{12}
\\\d{3}-\d{3}-\d{3}-\d{3}-\d
\I-\d{3}-\d{3}-\d{3}-\d{3}

Drivers License Number- FL. MI. MN States medium breadth **Table 34-66** validators

Mandator validator	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	fla, fl, florida, michigan, mi, minnesota, mn

### Drivers License Number- FL, MI, MN States wide breadth

The wide breadth edition of this data identifier detects any 13 character string with a letter followed by 12 numbers.

For the MN license number, the following format is matched: L-DDD-DDD-DDD-DDD.

Note: This breadth option does not include any validators.

**Table 34-67** Drivers License Number- FL, MI, MN States wide breadth patterns

#### **Patterns**

\\I \\d{3} \\d{3} \\d{3} \\d{3}

 $11d{12}$ 

 $\ld{3}-\d{$ 

 $I-d{3}-d{3}-d{3}$ 

# Drivers License Number- FL, MI, MN States medium breadth

The medium breadth edition of this data identifier implements patters to detect any 13 character string with a letter followed by 12 numbers. For the MN license number, the following format is matched: L-DDD-DDD-DDD.

This data identifier validates the number by requiring the presence of a drivers license keyword AND a state-related keyword.

Drivers License Number- FL, MI, MN States medium breadth patterns Table 34-68

Pattern	
\\\ \\d{3} \\d{3} \\d{3} \\d{3}	
\I\d{12}	
\ \d{3}-\d{3}-\d{2}-\d{3}-\d	
\I-\d{3}-\d{3}-\d{3}-\d{3}	

Table 34-69	Drivers License Number- FL, MI, MN States medium breadth
	validators

Mandator validator	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.

Table 34-69 Drivers License Number- FL, MI, MN States medium breadth validators (continued)

Mandator validator	Description
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	fla, fl, florida, michigan, mi, minnesota, mn

# Drivers License Number - IL State data identifier

This number is the identification number for an individual's driver's license issued by the US state of Illinois.

The Drivers License Number - IL State data identifier detects the presence of an Illinois drivers license number.

This data identifier provides two breadths of validation:

- The wide breadth edition detects the presence of a 12 character string. See "Drivers License Number- IL State wide breadth" on page 736.
- The medium breadth narrows the scope by requiring the presence of keywords. See "Drivers License Number- IL State medium breadth" on page 737.

#### Drivers License Number- IL State wide breadth

The wide breadth edition of the Drivers License Number- IL State data identifier detects a 12 character string, beginning with a letter (the first letter of the person's last name) followed by 11 numbers.

	Note: This breadth option does not include any validators.		
	Table 34-70	Drivers License Number- IL State wide breadth patterns	
Pattern			

\I\d{11}

\\I\\d{3}-\\d{4}-\\d{4}

#### Drivers License Number- IL State medium breadth

The medium breadth edition of the Drivers License Number- IL State data identifier detects a 12 character string, beginning with a letter (the first letter of the person's last name) followed by 11 numbers.

This breadth also requires the presence of both a driver's license keyword AND a Illinois-related keyword..

Table 34-71 Drivers License Number- IL State medium breadth patterns

Pattern	
\\\\d{3}-\\d{4}-\\d{4}	
\\\d{11}	

Drivers License Number- II. State medium breadth validators Table 34-72

Mandator validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	il, illinois

### Drivers License Number- II. State wide breadth

The wide breadth edition of the Drivers License Number- IL State data identifier detects a 12 character string, beginning with a letter (the first letter of the person's last name) followed by 11 numbers.

Note: This breadth option does not include any validators.

Table 34-73 Drivers License Number- IL State wide breadth patterns

#### Pattern

\\I\\d{3}-\\d{4}-\\d{4}

Table 34-73 Drivers License Number-IL State wide breadth patterns (continued)

P	٦t	٠	۵	rn

\I\d{11}

#### Drivers License Number- IL State medium breadth

The medium breadth edition of the Drivers License Number- IL State data identifier detects a 12 character string, beginning with a letter (the first letter of the person's last name) followed by 11 numbers.

This breadth also requires the presence of both a driver's license keyword AND a Illinois-related keyword..

Table 34-74 Drivers License Number- IL State medium breadth patterns

Pattern	
\\\\d{3}-\\d{4}-\\d{4}	
\\d{11}	

Drivers License Number- IL State medium breadth validators Table 34-75

Mandator validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	il, illinois

# Drivers License Number - NJ State data identifier

This number is the identification for an individual's driver's license issued by the US state of New Jersey.

The Drivers License Number - NJ State data identifier detects the presence of a New Jersey drivers license number.

This data identifier provides two breadths of validation:

- The wide breadth edition detects the presence of a 15 character string. See "Drivers License Number- NJ State wide breadth" on page 739.
- The medium breadth narrows the scope by requiring the presence of keywords. See "Drivers License Number- NJ State medium breadth" on page 739.

#### Drivers License Number- NJ State wide breadth

The wide breadth edition of the Drivers License Number- NJ State data identifier detects a 15 character string, beginning with a letter (the first letter of the person's last name) followed by 14 numbers.

Note: The wide breadth option does not include any validators.

Drivers License Number- NJ State wide breadth patterns **Table 34-76** 

### **Patterns**

\\I\\d{4} \\d{5} \\d{5}

 $11d{14}$ 

#### Drivers License Number- NJ State medium breadth

The medium breadth edition of the Drivers License Number- NJL State data identifier detects a 15 character string, beginning with a letter (the first letter of the person's last name) followed by 14 numbers.

This breadth also requires the presence of both a driver's license keyword AND a New Jersey-related keyword.

Drivers License Number- NJ State medium breadth patterns **Table 34-77** 

#### **Pattern**

\\I\\d{3}-\\d{4}-\\d{4}

\I\d{11}

**Table 34-78** Drivers License Number- NJ State medium breadth validators

Validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.

Table 34-78 Drivers License Number- NJ State medium breadth validators (continued)

Validators	Description
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	nj, new jersey, newjersey

#### Drivers License Number- NJ State wide breadth

The wide breadth edition of the Drivers License Number- NJ State data identifier detects a 15 character string, beginning with a letter (the first letter of the person's last name) followed by 14 numbers.

Note: The wide breadth option does not include any validators.

Table 34-79 Drivers License Number- NJ State wide breadth patterns

#### **Patterns**

\\I\\d{4} \\d{5} \\d{5}

 $11d{14}$ 

### Drivers License Number- NJ State medium breadth

The medium breadth edition of the Drivers License Number- NJL State data identifier detects a 15 character string, beginning with a letter (the first letter of the person's last name) followed by 14 numbers.

This breadth also requires the presence of both a driver's license keyword AND a New Jersey-related keyword.

Drivers License Number- NJ State medium breadth patterns Table 34-80

#### **Pattern**

\\I\\d{3}-\\d{4}-\\d{4}

\I\d{11}

Validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	nj, new jersey, newjersey

Table 34-81 Drivers License Number- NJ State medium breadth validators

# **Drivers License Number - NY State data identifier**

This number is the identification for an individual's driver's license issued by the US state of New York.

The Drivers License Number - NY State data identifier detects the presence of an New York drivers license number.

This data identifier provides two breadths of validation:

- The wide breadth edition detects a string of 9 digits. See "Drivers License Number- NJ State wide breadth" on page 739.
- The medium breadth narrows the scope by requiring the presence of keywords. See "Drivers License Number- NJ State medium breadth" on page 739.

#### Drivers License Number- NY State wide breadth

The wide breadth edition of the Drivers License Number- NY State data identifier detects a 9-digit string.

Note: The wide breadth option does not include any validators. Drivers License Number- NY State wide breadth patters Table 34-82

Pattern	
\\d{3} \\d{3} \\d{3}	
\d{9}	

#### Drivers License Number - NY State medium breadth

The medium breadth edition of the Drivers License Number - NY State data identifier detects a 9-digit string.

This breadth also requires the presence of both a driver's license keyword AND a New York-related keyword.

Table 34-83 Drivers License Number- NY State medium breadth patterns

Pattern	
\\\\d{3}-\\d{4}-\\d{4}	
\l\d{11}	

<b>Table 34-84</b> Drivers License Number- NY State mediun	breadth validators
--	--------------------

Mandatory validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	new york, ny, newyork

### Drivers License Number- NY State wide breadth

The wide breadth edition of the Drivers License Number- NY State data identifier detects a 9-digit string.

Note: The wide breadth option does not include any validators.

Table 34-85	Drivers License	Number- N\	/ State wide	breadth patters
-------------	-----------------	------------	--------------	-----------------

Pattern	
\\d{3} \\d{3} \\d{3}	
/d{9}	

#### Drivers License Number - NY State medium breadth

The medium breadth edition of the Drivers License Number - NY State data identifier detects a 9-digit string.

This breadth also requires the presence of both a driver's license keyword AND a New York-related keyword.

**Table 34-86** Drivers License Number- NY State medium breadth patterns

Pattern	
\\\\d{3}-\\d{4}-\\d{4}	
\l\d{11}	

Table 34-87	Drivers License Number-	<ul> <li>NY State medium breadth validators</li> </ul>
-------------	-------------------------	--

Mandatory validators	Description
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics#
Find keywords	Requires at least one of the input keywords or key phrases to be present for the data to be matched.
Find keywords input	new york, ny, newyork

# French INSEE Code data identifier

The INSEE code in France is used as a social insurance number, a national identification number, and for taxation and employment purposes.

The French INSEE Code data identifier detects the presence of INSEE numbers.

The wide breadth edition of the French INSEE Code data identifier detects a 15-digit number which encodes the date of birth, department of origin, commune of origin, and an order number. A space delimiter after the first 13 digits is optional. The last two digits of the INSEE code encode a control key used to validate a checksum.

**Table 34-88** French INSEE Code wide breadth patterns

	·
Pattern	
\d{13} \d{2}	

Table 34-88	Franch INISEE	Code wide bread	th nattarns	(continued)
1 abie 34-00	HEIICH INSEL	Code wide breat	illi palleilis	(Continueu)

Pattern	
d{15}	

Table 34-89	French INSEE Code wide breadth validator
-------------	--

Mandatory validator	Description
INSEE Control Key	This validator computes the INSEE control key and compares it to the last 2 digits of the pattern.

# Hong Kong ID data identifier

The Hong Kong ID is the unique identifier for all residents of Hong Kong and appears on the Hong Kong Identity Card.

The Hong Kong ID data identifier detects the presence of Hong Kong IDs.

The wide breadth edition of the Hong Kong ID data identifier detects 8 characters in the form LDDDDDD(D) or LDDDDDDD(A). The last character in the detected string is used to validate a checksum.

**Table 34-90** Hong Kong ID wide breadth patterns

Patterns	
\w\d{6}(\d)	
\w\d{6}(A)	
U\w\d{6}(\d)	
U\w\d{6}(A)	

Table 34-91 Hong Kong ID wide breadth validator

Mandatory validator	Description
Hong Kong ID	Computes the checksum and validates the pattern against it.

# **IBAN Central data identifier**

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN Central data identifier detects IBAN numbers for Andorra, Austria, Belgium, Germany, Italy, Liechtenstein, Luxembourg, Malta, Monaco, San Marino, and Switzerland.

The wide breadth edition of the IBAN Central data identifier detects a country-specfic IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

Table 34-92 IBAN Central wide breadth patterns

Pattern	Description
AD\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}	Andorra patterns
AD\d{2} \d{4} \d{4} \w{4} \w{4} \w{4}	
AD\d{2}-\d{4}-\d{4}-\w{4}-\w{4}	
AT\d{2}\d{4}\d{4}\d{4}\d{4}	Austria patterns
AT\d{2} \d{4} \d{4} \d{4} \d{4}	
AT\d{2}-\d{4}-\d{4}-\d{4}	
BE\d{2}\d{4}\d{4}\d{4}	Belgium patterns
BE\d{2} \d{4} \d{4} \d{4}	
BE\d{2}-\d{4}-\d{4}	
CH\d{2}\d{4}\d\w{3}\w{4}\w	Switzerland patterns
CH\d{2} \d{4} \d\w{3} \w{4} \w{4} \w	
CH\d{2}-\d{4}-\d\w{3}-\w{4}-\w{4}-\w	
DE\d{2}\d{4}\d{4}\d{4}\d{2}	Germany patterns
DE\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
DE\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	
IT\d{2}[A-Z]\d{3}\d{4}\d{3}\w\w{4}\w{4}\w{3}	Italy patterns
IT\d{2} [A-Z]\d{3} \d{4} \d{3}\w \w{4} \w{4} \w{3}	
$IT\d{2}-[A-Z]\d{3}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{3}$	
LI\d{2}\d{4}\d\w{3}\w{4}\w{4}\w	Liechtenstein patterns
LI\d{2} \d{4} \d\w{3} \w{4} \w{4} \w	
LI\d{2}-\d{4}-\d\w{3}-\w{4}-\w{4}-\w	

**Table 34-92** IBAN Central wide breadth patterns (continued)

Pattern	Description
LU\d{2}\d{3}\w\w{4}\w{4}\\w{4}	Luxembourg patterns
LU\d{2} \d{3}\w \w{4} \w{4} \w{4}	
LU\d{2}-\d{3}\w-\w{4}-\w{4}	
MC\d{2}\d{4}\d{2}\w{2}\w{4}\w{4}\w\d{2}	Monaco patterns
$MC\d{2} \d{4} \d{4} \d{2}\w{2} \w{4} \w{4} \w{4} \$	
$MC\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w{4}-\d{2}$	
MT\d{2}[A-Z]{4}\d{4}\d\w{3}\w{4}\w{4}\w{4}\w{3}	Malta
$ MT\d{2} [A-Z]{4} \d{4} \d\w{3} \w{4} \w{4} \w{4} \w{3} $	
$ MT\d{2}-[A-Z]{4}-\d{4}-\d{4}-\w{3}-\w{4}-\w{4}-\w{4}-\w{3}$	
SM\d{2}[A-Z]\d{3}\d{4}\d{3}\w\w{4}\w{4}\w{3}	San Marino patterns
$SM\d{2} [A-Z]\d{3} \d{4} \d{3}\w \w{4} \w{4} \w{3}$	
$SM\d{2}-[A-Z]\d{3}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{3}$	

Table 34-93 IBAN Central wide breadth validator

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

# IBAN East data identifier

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN East data identifier detects IBAN numbers for Bosnia, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Greece, Hungary, Israel, Latvia, Lithuania, Macedonia, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, Turkey and Tunisia.

The wide breadth IBAN East data identifier detects a country-specfic IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

**Table 34-94** IBAN East wide breadth patterns

Pattern	Description
BA\d{2}\d{4}\d{4}\d{4}\d{4}	Bosnia patterns
BA\d{2} \d{4} \d{4} \d{4} \d{4}	
BA\d{2}-\d{4}-\d{4}-\d{4}	
BG\d{2}[A-Z]{4}\d{4}\d{2}\w{2}\w{4}\w{2}	Bulgaria patterns
BG\d{2} [A-Z]{4} \d{4} \d{2}\w{2} \w{4} \w{2}	
BG\d{2}-[A-Z]{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{2}	
CY\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}\w{4}	Cyprus patterns
CY\d{2} \d{4} \d{4} \w{4} \w{4} \w{4} \w{4}	
CY\d{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}	
CZ\d{2}\d{4}\d{4}\d{4}\d{4}	Czech Republic patterns
CZ\d{2} \d{4} \d{4} \d{4} \d{4} \d{4}	
CZ\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
EE\d{2}\d{4}\d{4}\d{4}\d{4}	Estonia patterns
EE\d{2} \d{4} \d{4} \d{4} \d{4}	
EE\d{2}-\d{4}-\d{4}-\d{4}	
GR\d{2}\d{4}\d{3}\w\w{4}\w{4}\w{4}\w{3}	Greece patterns
GR\d{2} \d{4} \d{3}\w \w{4} \w{4} \w{4} \w{3}	
GR\d{2}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{4}-\w{3}	
HR\d{2}\d{4}\d{4}\d{4}\d	Croatia patterns
HR\d{2} \d{4} \d{4} \d{4} \d{4} \d	
HR\d{2}-\d{4}-\d{4}-\d{4}-\d	
HU\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	Hungary patterns
HU\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4}	
HU\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	
IL\d{2}\d{4}\d{4}\d{4}\d{3}	Israel patterns
IL\d{2} \d{4} \d{4} \d{4} \d{4} \d{3}	
IL\d{2}-\d{4}-\d{4}-\d{4}-\d{3}	

IBAN East wide breadth patterns (continued) **Table 34-94** 

Pattern	Description
LT\d{2}\d{4}\d{4}\d{4}\d{4}	Lithuania patterns
LT\d{2} \d{4} \d{4} \d{4}	
LT\d{2}-\d{4}-\d{4}-\d{4}	
LV\d{2}[A-Z]{4}\w{4}\w{4}\w	Latvia patterns
LV\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w	
LV\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w	
ME\d{2}\d{4}\d{4}\d{4}\d{2}	Montenegro patterns
ME\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
$ME\d{2}-\d{4}-\d{4}-\d{4}-\d{2}$	
MK\d{2}\d{3}\w\w{4}\w{4}\w\d{2}	Macedonia patterns
MK\d{2} \d{3}\w \w{4} \w{4} \w\d{2}	
$MK\d{2}-\d{3}\w-\w{4}-\w{4}-\w{4}$	
PL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	Poland patterns
PL\d{2} \d{4} \d{4} \d{4} \d{4} \d{4}	
PL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
RO\d{2}[A-Z]{4}\w{4}\w{4}\w{4}	Romania patterns
RO\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{4}	
RO\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}	
RS\d{2}\d{4}\d{4}\d{4}\d{2}	Serbia patterns
RS\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
RS\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	
SI\d{2}\d{4}\d{4}\d{3}	Slovenia patterns
SI\d{2} \d{4} \d{4} \d{4} \d{3}	
SI\d{2}-\d{4}-\d{4}-\d{4}-\d{3}	
SK\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	Slovak Republic patterns
SK\d{2} \d{4} \d{4} \d{4} \d{4}	
SK\d{2}-\d{4}-\d{4}-\d{4}	

**Table 34-94** IBAN East wide breadth patterns (continued)

Pattern	Description
TN59\d{4}\d{4}\d{4}\d{4}\d{4}	Tunisia patterns
TN59 \d{4} \d{4} \d{4} \d{4} \d{4}	
TN59-\d{4}-\d{4}-\d{4}-\d{4}	
TR\d{2}\d{4}\d\w{3}\w{4}\w{4}\w{2}	Turkey patterns
TR\d{2} \d{4} \d\w{3} \w{4} \w{4} \w{4} \w{2}	
$TR\d{2}-\d{4}-\d{w}{3}-\w{4}-\w{4}-\w{4}-\w{2}$	

IBAN East wide breadth validator Table 34-95

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

# IBAN West data identifier

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN West data identifier detects IBAN numbers for Denmark, Faroe Islands, Finland, France, Gibraltar, Greenland, Iceland, Ireland, Netherlands, Norway, Portugal, Spain, Sweden, and the United Kingdom.

The wide breadth IBAN West data identifier detects a country-specfic IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

Table 34-96 IBAN West wide breadth patterns

Pattern	Description
DK\d{2}\d{4}\d{4}\d{2}	Denmark patterns
DK\d{2} \d{4} \d{4} \d{4} \d{2}	
DK\d{2}-\d{4}-\d{4}-\d{4}	
ES\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	Spain patterns
ES\d{2} \d{4} \d{4} \d{4} \d{4}	
ES\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	

**Table 34-96** IBAN West wide breadth patterns (continued)

Pattern	Description
FI\d{2}\d{4}\d{4}\d{2}	Finland patterns
FI\d{2} \d{4} \d{4} \d{4} \d{2}	
FI\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	
FO\d{2}\d{4}\d{4}\d{2}	Faroe Islands patterns
FO\d{2} \d{4} \d{4} \d{4} \d{2}	
FO\d{2}-\d{4}-\d{4}-\d{2}	
FR\d{2}\d{4}\d{4}\d{2}\w{2}\w{4}\w{4}\w\d{2}	France patterns
FR\d{2} \d{4} \d{4} \d{2}\w{2} \w{4} \w{4} \w\d{2}	
FR\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w\d{2}	
GB\d{2}[A-Z]{4}\d{4}\d{4}\d{2}	United Kingdom
GB\d{2} [A-Z]{4} \d{4} \d{4} \d{2}	
GB\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	
GI\d{2}[A-Z]{4}\w{4}\w{4}\w{3}	Gibraltar patterns
GI\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{3}	
GI\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{3}	
GL\d{2}\d{4}\d{4}\d{4}\d{2}	Greenland patterns
GL\d{2} \d{4} \d{4} \d{4} \d{2}	
GL\d{2}-\d{4}-\d{4}-\d{2}	
IE\d{2}[A-Z]{4}\d{4}\d{4}\d{2}	Ireland patterns
IE\d{2} [A-Z]{4} \d{4} \d{4} \d{4} \d{2}	
IE\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	
IS\d{2}\d{4}\d{4}\d{4}\d{4}\d{2}	Iceland patterns
IS\d{2} \d{4} \d{4} \d{4} \d{4} \d{2}	
IS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	
NL\d{2}[A-Z]{4}\d{4}\d{4}\d{2}	Netherlands patterns
NL\d{2} [A-Z]{4} \d{4} \d{4} \d{2}	
NL\d{2}-[A-Z]{4}-\d{4}-\d{2}	

**Table 34-96** IBAN West wide breadth patterns (continued)

Pattern	Description
NO\d{2}\d{4}\d{4}\d{3}	Montenegro patterns
NO\d{2} \d{4} \d{4} \d{3}	
NO\d{2}-\d{4}-\d{4}-\d{3}	
PT\d{2}\d{4}\d{4}\d{4}\d{4}\d	Portugal patterns
PT\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d	
PT\d{2}-\d{4}-\d{4}-\d{4}-\d	
SE\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}	Sweden patterns
SE\d{2} \d{4} \d{4} \d{4} \d{4} \d{4}	
SE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	

IBAN West wide breadth validator **Table 34-97** 

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

# IP Address data identifier

An IP address is the computer networking code that is used to identify devices and facilitate communications.

The IP Address data identifier detects IP addresses.

This data identifier offers three breadths of detection:

- Wide See "IP Address wide breadth" on page 752.
- Medium See "IP Address medium breadth" on page 753.
- Narrow See "IP Address narrow breadth" on page 754.

Note: The patterns for the IP Address data identifier are tuned to match IPv4 address formats. You can create a custom data identifier to detect IPv6 address formats. See "About IPv6 support for Network Monitor" on page 1143.

#### IP Address wide breadth

The wide breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed.

**Table 34-98** IP Address wide breadth patterns

Pattern
d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]
d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?
d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

**Table 34-99** IP Address wide breadth validator

Validator	Description
IP Basic Check	Every IP address must match the format x.x.x.x and every number must be less than 256.

#### IP Address medium breadth

The medium breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed. Also, eliminates as common fictitious examples all 1-digit match groups such as 1.1.1.2.

IP Address medium breadth patterns Table 34-100

Pattern
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}}[3][0-2]?

Table 34-101 IP Address medium breadth validator

Mandatory Validator	Description
IP Octet Check	Every IP address must match the format x.x.x.x, every number must be less than 256, and no IP address can contain only single-digit numbers (1.1.1.2).

#### IP Address narrow breadth

The narrow breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed. Also, eliminates as common fictitious examples all 1-digit match groups such as 1.1.1.2. Also eliminates unassigned IP addresses ("bogons").

Table 34-102 IP Address medium breadth patterns

Pattern	
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}	
\d{1,3}.\d{1,3}.\d{1,3}\.\d{1,3}\[0-9]	
\d{1,3}.\d{1,3}.\d{1,3}\.1,	
\d{1,3}.\d{1,3}.\d{1,3}\\d{1,3}}[3][0-2]?	

Table 34-103 IP Address wide breadth validator

Mandatory Validator	Description
IP Octet Check	Every IP address must match the format x.x.x.x, every number must be less than 256, and no IP address can contain only single-digit numbers (1.1.1.2).
IP Octet Check	Checks whether the IP address falls into any of the "Bogons" ranges. If so the match is invalid.

### IP Address wide breadth

The wide breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed.

Table 34-104 IP Address wide breadth patterns

Pattern	
\d{1,3}.\d{1,3}.\d{1,3}	
\d{1,3}.\d{1,3}.\d{1,3}}[0-9]	
\d{1,3}.\d{1,3}.\d{1,3}}[0-9]?	
\d{1,3}.\d{1,3}.\d{1,3}\.\d{1,3}}[0-2]?	

IP Address wide breadth validator Table 34-105

Validator	Description
IP Basic Check	Every IP address must match the format x.x.x.x and every number must be less than 256.

# IP Address medium breadth

The medium breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed. Also, eliminates as common fictitious examples all 1-digit match groups such as 1.1.1.2.

**Table 34-106** IP Address medium breadth patterns

Pattern	
\d{1,3}.\d{1,3}.\d{1,3}	
\d{1,3}.\d{1,3}.\d{1,3}\\d{1,3}\\d\d	
\d{1,3}.\d{1,3}.\d{1,3}\[1-2][0-9]?	
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?	

IP Address medium breadth validator Table 34-107

Mandatory Validator	Description
IP Octet Check	Every IP address must match the format x.x.x.x, every number must be less than 256, and no IP address can contain only single-digit numbers (1.1.1.2).

#### IP Address narrow breadth

The narrow breadth edition of the IP Address data identifier detects numbers in format DDD.DDD.DDD.DDD with an optional /DD. Each three digit group must be between 0 and 255 inclusive and the /DD must be between 0 and 32. Additionally, 0.0.0.0 is not allowed. Also, eliminates as common fictitious examples all 1-digit match groups such as 1.1.1.2. Also eliminates unassigned IP addresses ("bogons").

Table 34-108 IP Address medium breadth patterns

Pattern
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
\d{1,3}.\d{1,3}.\d{1,3}\.\d{1,3}\/[0-9]
\d{1,3}.\d{1,3}.\d{1,3}\.1,
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

Table 34-109 IP Address wide breadth validator

Mandatory Validator	Description
IP Octet Check	Every IP address must match the format x.x.x.x, every number must be less than 256, and no IP address can contain only single-digit numbers (1.1.1.2).
IP Octet Check	Checks whether the IP address falls into any of the "Bogons" ranges. If so the match is invalid.

# National Drug Code (NDC) data identifier

The National Drug Code (NDC) is an identifier issued by the Food and Drug Administration (FDA) for an individual drug in the United States. An alternate format is defined by HIPAA regulations.

The National Drug Code data identifier detects the existence of an NDC as well as the HIPAA version.

This data identifier provides three breadths of detection:

- The wide breadth checks for the existence of an NDC number or its HIPAA version.
  - See "Drivers License Number- FL, MI, MN States wide breadth" on page 734.
- The medium breadth restricts the patterns for detecting the numbers. See "Drivers License Number-FL, MI, MN States medium breadth" on page 734.
- The narrow breadth requires a keyword match.

See "Drivers License Number- FL, MI, MN States medium breadth" on page 734.

# National Drug Code (NDC) wide breadth

The wide breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes or spaces.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit.

Table 34-110 National Drug Code (NDC) wide breadth patterns

Patterns
*?\d{4} \d{4} \d{2}
*?\d{4}-\d{2}
\d{5} *?\d{3} \d{2}
\d{5}-*?\d{3}-\d{2}
\d{5} \d{4} *?\d
\d{5}-\d{4}-*?\d
\d{5} \d{4} \d{2}
\d{5}-\d{4}-\d{2}

# National Drug Code (NDC) medium breadth

The medium breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit.

**Note:** The medium edition of this data identifier does not include any validators.

Note: The wide breadth edition of this data identifier allows for the NDC number to be space-delimited; the medium breadth edition does not. That is the difference between the wide and medium editions of this data identifier.

**Table 34-111** National Drug Code (NDC) medium breadth patterns

Pattern	
?\d{4}-\d{4}-\d{2}	
d{5}-*?\d{3}-\d{2}	
d{5}-\d{4}-*?\d	
d{5}-\d{4}-\d{2}	

# National Drug Code (NDC) narrow breadth

The narrow breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit. This data identifier also requires the presence of an NDC-related keyword.

Table 34-112 National Drug Code (NDC) narrow breadth patterns

Pattern
*?\d{4}-\d{2}
\d{5}-*?\d{3}-\d{2}
\d{5}-\d{4}-*?\d
\d{5}-\d{4}-\d{2}

**Table 34-113** National Drug Code (NDC) narrow breadth validators

Mandatory validator	Description
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	ndc, national drug code

# National Drug Code (NDC) wide breadth

The wide breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes or spaces.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit.

Table 34-114 National Drug Code (NDC) wide breadth patterns

atterns	
?\d{4} \d{4} \d{2}	
?\d{4}-\d{4}-\d{2}	
d{5} *?\d{3} \d{2}	
d{5}-*?\d{3}-\d{2}	
d{5} \d{4} *?\d	
d{5}-\d{4}-*?\d	
d{5} \d{4} \d{2}	
d{5}-\d{4}-\d{2}	

# National Drug Code (NDC) medium breadth

The medium breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit.

Note: The medium edition of this data identifier does not include any validators.

Note: The wide breadth edition of this data identifier allows for the NDC number to be space-delimited; the medium breadth edition does not. That is the difference between the wide and medium editions of this data identifier.

National Drug Code (NDC) medium breadth patterns Table 34-115

Pattern			
*?\d{4}-\d{4}-\d{2}			
\d{5}-*?\d{3}-\d{2}			
\d{5}-\d{4}-*?\d			

Table 34-115 National Drug Code (NDC) medium breadth patterns (continued)

Р	-	+	+	^	,	n

\d{5}-\d{4}-\d{2}

## National Drug Code (NDC) narrow breadth

The narrow breadth edition of the National Drug Code (NDC) data identifier detects the standard FDA format, which is a 10-digit number in the format 4-4-2, 5-4-1 or 5-3-2, with the numbers separated by dashes.

This data identifier also detects the HIPAA format, an 11-digit number in the format 5-4-2. The HIPAA format may include a single asterisk to represent a missing digit. This data identifier also requires the presence of an NDC-related keyword.

National Drug Code (NDC) narrow breadth patterns Table 34-116

Pattern
*?\d{4}-\d{2}
\d{5}-*?\d{3}-\d{2}
\d{5}-\d{4}-*?\d
\d{5}-\d{4}-\d{2}

Table 34-117 National Drug Code (NDC) narrow breadth validators

Mandatory validator	Description
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	ndc, national drug code

# People's Republic of China ID data identifier

The People's Republic of China ID is used for residential registration, army enrollment registration, registration of marriage/divorce, traveling abroad, taking part in various national exams, and other social or civil matters in China.

The People's Republic of China ID data identifier detects the presence of this 18-digit number.

The wide breadth edition of the People's Republic of China ID data identifier detects an 18-digit number with the last number being used to validate a checksum.

Table 34-118	People's Republic of China ID wide breadth pat	terns
--------------	--	-------

Pattern				
\d{17}[Xx]				
\d{18}				
Table 34-119 People's Republic of China ID wide breadth validator				
Mandatory validator	Description			
China ID checksum validator	Computes the checksum and validates the pattern against it.			

# Randomized US Social Security Number (SSN) data identifier

The Randomized US Social Security Number (SSN) data identifier detects 9-digit numbers with the pattern DDD-DDDDD, separated with dashes or spaces or without separators. The number must be in valid assigned number ranges. Pattern validators eliminate common test numbers, such as 123456789 or all the same digit. The data identifier is narrow in breadth and requires the presence of a Social Security-related keyword.

In Symantec Data Loss Prevention version 12.5, the Randomized US SSN data identifier replaces the US Social Security Number (SSN) data identifier. All policy templates that implement the US SSN data identifier are updated to use the system-defined Randomized US SSN data identifier. In addition, in version 12.5 the patterns and validators for the Randomized US SSN data identifier are updated from the 12.0 version of the Randomized US SSN data identifier. Symantec recommends that you update your policies to use the version 12.5 Randomized US SSN data identifier.

See "Updating policies to use the Randomized US SSN data identifier" on page 569.

See "Use the Randomized US SSN data identifier to detect SSNs" on page 582.

Table 34-120 lists the patterns and normalizer used by the Randomized US SSN data identifier.

Component	Value	Description
Patterns	[0-8]\d{2}\d{1}[1-9]\d{4} [0-8]\d{3}[1-9]\d{4} [0-8]\d{2}[1-9]\d{5} [0-8]\d{2}-\d{1}[1-9]-\d{4} [0-8]\d{2} [1-9]\d{1}\d{4} [0-8]\d{2}-[1-9]\d{1}-\d{4}	Detects 9-digit numbers with the pattern DDD-DD-DDDD, separated with dashes, spaces, or none. The number must be in valid assigned number ranges
Data Normalizer	Digits	See "About data normalizers" on page 548.

Table 34-120 Randomized US SSN patterns and normalizer

Table 34-121 lists the validators and data input used for the Randomized US SSN data identifier.

Active Validators	Input (if any)	Description
Exclude beginning characters	666, 000, 123456789, 1111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 77777777, 888888888	See "Using pattern validators" on page 575.
Number Delimiter		
Exclude ending characters	0000	

social security number, ssn, ss#

Table 34-121 Randomized US SSN validators and input

# Singapore NRIC data identifier

Find keywords

The Singapore NRIC (National Registration Identity Card) is the identity document used in Singapore. The NRIC is a required document for some government procedures, commercial transactions such as the opening of a bank account, or to gain entry to premises by surrendering or exchanging for an entry pass.

The wide breadth edition of the Singapore NRIC data identifier detects 9 characters in the pattern LDDDDDDDL. The last character is used to validate a checksum.

Table 2/L122	Singanoro	NRIC wide	broadth	nattorn
Table 34-122	Sillgapore	NRIC WIGE	breautii	pattern

Pattern			
[SFTGsftg]\d{7}\w			
Table 34-123         Singapore NRIC wide breadth validator			
Mandatory validator	Description		
Singapore NRIC	Computes the Singapore NRIC checksum and validates the pattern against it.		

# South Korea Resident Registration Number data identifier

The South Korea Resident Registration Number is a 13-digit number issued to all residents of the Republic of Korea. Similar to national identification numbers in other countries, it is used to identify people in various private transactions such as in banking and employment. It is also used extensively for online identification purposes.

The South Korea Resident Registration Number data identifier detects the presence of this 13-digit number.

This data identifier provides two breadths of validation:

- The wide breadth edition matches numbers with dash delimiters or no delimiters. See "South Korea Resident Registration Number wide breadth" on page 762.
- The medium breadth edition matches a dash-delimited number only. See "South Korea Resident Registration Number medium breadth" on page 763.

This data identifier does not provide a narrow breadth option.

### South Korea Resident Registration Number wide breadth

The wide breadth edition of the South Korea Resident Registration Number data identifier detects 13 numeric characters that contain encoded birth date, gender, and origin of birth. It matches with dash or no delimiters, and validates the pattern using a checksum.

Table 34-124 South Korea Resident Registration Number wide breadth patterns

Pattern	
\d{2}[01]\d[0123]\d{8}	
\d{2}[01]\d[0123]\d-\d{7}	

South Korea Resident Registration Number wide breadth validators Table 34-125

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding numbers.
Advanced KRRN Validation	Validates that the 3rd and 4th digit are a valid month, that the 5th and 6th digit are a valid day, and the checksum matches the check digit.

## South Korea Resident Registration Number medium breadth

The medium breadth edition of the South Korea Resident Registration Number data identifier detects 13 numeric characters that contain encoded birth date, gender, and origin of birth, also validates the pattern using a checksum. This pattern requires a dash delimiter.

Table 34-126 South Korea Resident Registration Number medium breadth pattern

Pattern		
\d\d[01]\d[0123]\d-\d{7}		

South Korea Resident Registration Number medium breadth Table 34-127 validators

Validator	Description
Number Delimiter	Validates a match by checking the surrounding numbers.
Advanced KRRN Validation	Validates that the 3rd and 4th digit are a valid month, that the 5th and 6th digit are a valid day, and the checksum matches the check digit.

### South Korea Resident Registration Number wide breadth

The wide breadth edition of the South Korea Resident Registration Number data identifier detects 13 numeric characters that contain encoded birth date, gender, and origin of birth. It matches with dash or no delimiters, and validates the pattern using a checksum.

Table 34-128 South Korea Resident Registration Number wide breadth patterns

Pattern	
\d{2}[01]\d[0123]\d{8}	
\d{2}[01]\d[0123]\d-\d{7}	

South Korea Resident Registration Number wide breadth validators Table 34-129

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding numbers.
Advanced KRRN Validation	Validates that the 3rd and 4th digit are a valid month, that the 5th and 6th digit are a valid day, and the checksum matches the check digit.

## South Korea Resident Registration Number medium breadth

The medium breadth edition of the South Korea Resident Registration Number data identifier detects 13 numeric characters that contain encoded birth date, gender, and origin of birth, also validates the pattern using a checksum. This pattern requires a dash delimiter.

Table 34-130 South Korea Resident Registration Number medium breadth pattern

Pattern		
\d\d[01]\d[0123]\d-\d{7}		

South Korea Resident Registration Number medium breadth Table 34-131 validators

Validator	Description
Number Delimiter	Validates a match by checking the surrounding numbers.
Advanced KRRN Validation	Validates that the 3rd and 4th digit are a valid month, that the 5th and 6th digit are a valid day, and the checksum matches the check digit.

# Spanish DNI ID data identifier

The Spanish DNI ID number appears on the Documento nacional de identidad (DNI) and is issued by the Spanish Hacienda Publica to every citizen of Spain. It is the most important unique identifier used in Spain used for opening accounts, signing contracts, taxes, and elections.

The wide breadth edition of the Spanish DNI ID data identifier detects an 8-digit number followed by a hyphen and letter. Optionally the letter X and a hyphen can appear at the beginning for foreign nationals. The last letter must match a checksum algorithm.

Table 34-132 Spanish DNI ID wide breadth patterns

Pattern		
\d{8}-\w		
X-\d{8}-\w		
	 6	

Table 34-133 Spanish DNI ID wide breadth validator

Mandatory validator	Description
DNI control key check	Computes the control key and checks if it is valid.

# SWIFT Code data identifier

The SWIFT Code is a unique identifier for a banks and is managed by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). The SWIFT Code is required for monetary transfers between financial institutions. It is also known as the Bank Identifier Code (BIC).

The SWIFT Code data identifier detects the presence of the SWIFT Code.

This data identifier provides two breadths of validation:

- Wide breadth See "SWIFT Code wide breadth" on page 766.
- Narrow breadth See "SWIFT Code narrow breadth" on page 766.

### SWIFT Code wide breadth

The wide breadth edition of the SWIFT Code data identifier detects Detects 8- or 11-character strings. The 5th and 6th characters are the country code. This breadth also requires presence of a SWIFT-related keyword.

Table 34-134 SWIFT Code wide breadth patterns

Pattern	
[A-Z]{6}\w{2}	

Table 34-134 SWIFT Code wide breadth patterns (continued)

Pattern		
[A-Z]{6}\w{5}		

SWIFT Code wide breadth validators Table 34-135

Mandatory validator	Description
Require beginning characters	With this option selected, any of the following list of values are required at the beginning of the matched data.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	bic, bic#, international organization for standardization 9362, iso 9362, iso 9362, swift, swift#, swiftcode, swiftnumber, swiftroutingnumber.

#### SWIFT Code narrow breadth

The narrow breadth edition of the SWIFT Code data identifier detects 8- or 11-character strings. The 5th and 6th characters are letters referring to a country code. This breadth also requires presence of specific SWIFT-related keywords.

Table 34-136 SWIFT Code narrow breadth patterns

Pattern	
[A-Z]{6}\w{2}	
[A-Z]{6}\w{5}	

SWIFT Code narrow breadth validators Table 34-137

Validator	Description
Require beginning characters	With this option selected, any of the following list of values are required at the beginning of the matched data.
Find keywords	With this option selected, at least one of the following keywords or keyphrases must be present for the data to be matched.
Find keywords input	bic#, international organization for standardization 9362, iso 9362, iso 9362, swift#, swiftcode, swiftnumber, swiftroutingnumber, swift code, swift number, swift routing number, bic number, bic code, bic #

#### SWIFT Code wide breadth

The wide breadth edition of the SWIFT Code data identifier detects Detects 8- or 11-character strings. The 5th and 6th characters are the country code. This breadth also requires presence of a SWIFT-related keyword.

SWIFT Code wide breadth patterns Table 34-138

Pattern	
[A-Z]{6}\w{2}	
[A-Z]{6}\w{5}	

SWIFT Code wide breadth validators Table 34-139

Mandatory validator	Description
Require beginning characters	With this option selected, any of the following list of values are required at the beginning of the matched data.
Find keywords	With this option selected, at least one of the following keywords or key phrases must be present for the data to be matched.
Find keywords input	bic, bic#, international organization for standardization 9362, iso 9362, iso 9362, swift, swift#, swiftcode, swiftnumber, swiftroutingnumber.

#### SWIFT Code narrow breadth

The narrow breadth edition of the SWIFT Code data identifier detects 8- or 11-character strings. The 5th and 6th characters are letters referring to a country code. This breadth also requires presence of specific SWIFT-related keywords.

**Table 34-140** SWIFT Code narrow breadth patterns

Pattern			
[A-Z]{6}\w{2}			
[A-Z]{6}\w{5}			

SWIFT Code narrow breadth validators Table 34-141

Validator	Description
Require beginning characters	With this option selected, any of the following list of values are required at the beginning of the matched data.

Validator	Description
Find keywords	With this option selected, at least one of the following keywords or keyphrases must be present for the data to be matched.
Find keywords input	bic#, international organization for standardization 9362, iso 9362, iso 9362, swift#, swiftcode, swiftnumber, swiftroutingnumber, swift code, swift number, swift routing number, bic number, bic code, bic #

Table 34-141 SWIFT Code narrow breadth validators (continued)

# Swiss AHV Number data identifier

In Switzerland the Old Age and Survivors Insurance Fund number (Alters- und Hinterlassenenversicherungsnummer - AHV number) is the most important public ID number.

The Swiss AHV Number data identifier detects the 11-digit identifier with or without the standard period delimiter (DDD.DDD.DDD) and is validated against a checksum algorithm.

Table 34-142 Swiss AHV Number wide breadth patterns

Pattern			
\d{8}-\w			
X-\d{8}-\w			

Swiss AHV Number wide breadth validators Table 34-143

Validator	Description
Swiss AHV	Swiss AHV Modulus 11 Checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.

# Taiwan ID data identifier

In Taiwan an ID card is mandatory for all citizens who are over 14-years old. The ID card has been uniformly numbered since 1965.

The Taiwan ID data identifier detects the presence of Taiwan identification number based on two types of comon ID patterns. The last character matched is used to validate a checksum.

Table 34-144	Taiwan	ID wide	breadth	nattern
14DIE 34-144	Talwall	ID WIGE	breaum	Dattern

Patterns				
[A-Z][12][0-3]\d{7}				
[A-Z][ABCD]\d{8}				
Table 34-145 Taiwan ID wide breadth validator				
Validator			Description	
Taiwan ID			Taiwan ID checksum.	

## **UK Drivers License Number data identifier**

The UK Drivers License Number is the identification number for an individual's driver's license issued by the Driver and Vehicle Licensing Agency of the United Kingdom.

The UK Drivers License Number data identifier detects the presence of UK Drivers License numbers.

This data identifier provides three breadths of validation:

- Wide See "UK Drivers License Number wide breadth" on page 770.
- Medium See "UK Drivers License Number medium breadth" on page 770.
- Narrow See "UK Drivers License Number narrow breadth" on page 771.

### UK Drivers License Number wide breadth

The wide breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D a digit, and L a letter.

Note: This breadth option does not include any validators.

Table 34-146 UK Drivers License Number wide breadth patterns

Pattern	
\w{5}\d[0156]\d{4}\w{3}\l{2}	
\w{5} \d[0156]\d{4} \w{3}\l{2}	

#### UK Drivers License Number medium breadth

The medium breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D a digit, and L a letter.

The first digit in the numeric section is restricted to 0,1,5, or 6. In addition, the 4th and 5th digits in the numeric section must be between 01 and 31, inclusive.

Table 34-147 UK Drivers License Number medium breadth patterns

Pattern	
\w{5}\d[0156]\d{4}\w{3}\l{2}	
\w{5} \d[0156]\d{4} \w{3}\l{2}	

Table 34-148 UK Drivers License Number medium breadth validator

Mandatory validator	Description	
UK Drivers License	Every UK drivers license must be 16 characters and the number at the 8th and 9th position must be larger than 00 and smaller than 32.	

# UK Drivers License Number narrow breadth

The narrow breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D is a digit, and L is a letter.

The first digit is restricted to 0,1,5, or 6. In addition, the 4th and 5th digits in the numeric section must be between 01 and 31, inclusive.

In addition, the narrow breadth edition also requires the presence of both a driver's license-related keyword AND a UK-related keyword.

Table 34-149 UK Drivers License Number narrow breadth patterns

Pattern	
\w{5}\d[0156]\d{4}\w{3}\l{2}	
\w{5} \d[0156]\d{4} \w{3}\\{2}	

UK Drivers License Number narrow breadth validators Table 34-150

Mandatory validator	Description
UK Drivers License	Every UK drivers license must be 16 characters and the number at the 8th and 9th position must be larger than 00 and smaller than 32.
Find keywords: driver's license-related	At least one of the following keywords or key phrases must be present for the data to match: british, the united kingdom, uk, united kingdom, unitedkingdom
Find keywords: UK-related	At least one of the following keywords or keyphrases must be present for the data to match: british, the united kingdom, uk, united kingdom, unitedkingdom

#### UK Drivers License Number wide breadth

The wide breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D a digit, and L a letter.

Note: This breadth option does not include any validators.	

Table 34-151	UK Drivers	License Numb	oer wide	breadth	patterns
--------------	------------	--------------	----------	---------	----------

Pattern
\w{5}\d[0156]\d{4}\w{3}\\{2}
\w{5} \d[0156]\d{4} \w{3}\l{2}

### UK Drivers License Number medium breadth

The medium breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D a digit, and L a letter.

The first digit in the numeric section is restricted to 0,1,5, or 6. In addition, the 4th and 5th digits in the numeric section must be between 01 and 31, inclusive.

Table 34-152 UK Drivers License Number medium breadth patterns

Pattern	
\w{5}\d[0156]\d{4}\w{3}\l{2}	}
\w{5} \d[0156]\d{4} \w{3}\l{2}	2}

**Table 34-153** UK Drivers License Number medium breadth validator

Mandatory validator	Description
UK Drivers License	Every UK drivers license must be 16 characters and the number at the 8th and 9th position must be larger than 00 and smaller than 32.

#### UK Drivers License Number narrow breadth

The narrow breadth edition of the UK Drivers License Number data identifier detects 16 character strings of the following format: AAAAAD[0,1,5,6]DDDDAAALL, where A is an alphanumeric character, D is a digit, and L is a letter.

The first digit is restricted to 0,1,5, or 6. In addition, the 4th and 5th digits in the numeric section must be between 01 and 31, inclusive.

In addition, the narrow breadth edition also requires the presence of both a driver's license-related keyword AND a UK-related keyword.

Table 34-154 UK Drivers License Number narrow breadth patterns

Pattern	
\w{5}\d[0156]\d{4}\w{3}\l{2}	
\w{5} \d[0156]\d{4} \w{3}\\{2}	

Table 34-155 UK Drivers License Number narrow breadth validators

Mandatory validator	Description
UK Drivers License	Every UK drivers license must be 16 characters and the number at the 8th and 9th position must be larger than 00 and smaller than 32.
Find keywords: driver's license-related	At least one of the following keywords or key phrases must be present for the data to match:
	british, the united kingdom, uk, united kingdom, unitedkingdom

Table 34-155 UK Drivers License Number narrow breadth validators (continued)

Mandatory validator	Description
Find keywords: UK-related	At least one of the following keywords or keyphrases must be present for the data to match:
	british, the united kingdom, uk, united kingdom, unitedkingdom

## **UK Electoral Roll Number data identifier**

The Electoral Roll Number is the identification number issued to an individual for UK election registration. The format of this number is specified by the UK Government Standards of the UK Cabinet Office.

The UK Electoral Roll Number data identifier detects the presence of UK Electoral Roll Number. It implements a pattern to detect strings consisting of 2 to 3 letters, followed by 1 to 4 digits.

Table 34-156 UK Electoral Roll Number wide breadth pattern

Р	-	+	٠	^	r	n

 $I{2,3}d{1,4}$ 

The wide breadth edition of the Electoral Roll Number data identifier implements two validators to require the presence of an electoral number-related keyword and a UK-reated keyword.

UK Flectoral Roll Number wide breadth validators Table 34-157

Validator	Description
Find keywords: electoral number-related	At least one of the following keywords or key phrases must be present for the data to match:
	electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoral roll#, electoral#, electoralnumber, electoralroll#, electoralrollno
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:
	british, the united kingdom, uk, united kingdom, unitedkingdom

# **UK National Health Service (NHS) Number data** identifier

The UK National Health Service (NHS) Number is the personal identification number issued by the U.K. National Health Service (NHS) for administration of medical care.

The UK National Health Service (NHS) Number data identifier detects the presence of the UK National Health Service (NHS) Number.

This data identifier provides two breadths of validation:

- Medium See "UK National Health Service (NHS) Number medium breadth" on page 775.
- Narrow See "UK National Health Service (NHS) Number narrow breadth" on page 776.

Note: This data identifier does not provide a wide breadth option.

# UK National Health Service (NHS) Number medium breadth

The medium breadth edition of the UK National Health Service (NHS) Number data identifier implements patterns to detect numbers in the currently defined NHS format, DDD-DDDD (where D is a digit), with various separators.

Table 34-158 UK National Health Service (NHS) Number medium breadth patterns

Pattern	Description
\d{3}.\d{3}.\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by periods.
\d{3} \d{3} \d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by spaces.
\d{3}-\d{3}-\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by dashes.

The medium breadth edition of the UK National Health Service (NHS) Number data identifier implements three validators: one to validate the NHS checksum, another to perform numerical validation using the final digit, and a third to check for the presence of an NHS-related keyword.

Table 34-159 UK National Health Service (NHS) Number medium breadth validators

Validator	Description
UK NHS	UK NHS checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.
Find keywords: NHS-related	At least one of the following keywords or key phrases must be present for the data to match:  national health service, NHS

## UK National Health Service (NHS) Number narrow breadth

The narrow breadth edition of the UK National Health Service (NHS) Number data identifier implements patterns to detect numbers in the currently defined format: DDD-DDDD (where D is a digit), separated with dashes, spaces, or periods.

Table 34-160 UK National Health Service (NHS) Number narrow breadth patterns

Pattern	Description
\d{3}.\d{3}.\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by periods.
\d{3} \d{3} \d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by spaces.
\d{3}-\d{3}-\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by dashes.

The narrow breadth edition of the UK National Health Service (NHS) Number data identifier implements four validators: one to validate the NHS checksum, another to perform numerical validation using the final digit, a third to require the presence of an NHS-related keyword, and a fourth to require the presence of a UK-related keyword.

Table 34-161 UK National Health Service (NHS) Number narrow breadth validators

Mandatory validator	Description
UK NHS	UK NHS checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.

Table 34-161 UK National Health Service (NHS) Number narrow breadth validators (continued)

Mandatory validator	Description
Find keywords: NHS-related	At least one of the following keywords or key phrases must be present for the data to match:  national health service, NHS
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:  uk, united kingdom, britain, england, gb

### UK National Health Service (NHS) Number medium breadth

The medium breadth edition of the UK National Health Service (NHS) Number data identifier implements patterns to detect numbers in the currently defined NHS format, DDD-DDD-DDDD (where D is a digit), with various separators.

Table 34-162 UK National Health Service (NHS) Number medium breadth patterns

Pattern	Description
\d{3}.\d{3}.\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by periods.
\d{3} \d{3} \d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by spaces.
\d{3}-\d{3}-\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by dashes.

The medium breadth edition of the UK National Health Service (NHS) Number data identifier implements three validators: one to validate the NHS checksum, another to perform numerical validation using the final digit, and a third to check for the presence of an NHS-related keyword.

UK National Health Service (NHS) Number medium breadth Table 34-163 validators

Validator	Description
UK NHS	UK NHS checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.

Table 34-163 UK National Health Service (NHS) Number medium breadth validators (continued)

Validator	Description
Find keywords: NHS-related	At least one of the following keywords or key phrases must be present for the data to match:
	national health service, NHS

#### UK National Health Service (NHS) Number narrow breadth

The narrow breadth edition of the UK National Health Service (NHS) Number data identifier implements patterns to detect numbers in the currently defined format: DDD-DDDD (where D is a digit), separated with dashes, spaces, or periods.

Table 34-164 UK National Health Service (NHS) Number narrow breadth patterns

Pattern	Description
\d{3}.\d{3}.\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by periods.
\d{3} \d{3} \d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by spaces.
\d{3}-\d{3}-\d{4}	Pattern for detecting the format DDD-DDD-DDDD separated by dashes.

The narrow breadth edition of the UK National Health Service (NHS) Number data identifier implements four validators: one to validate the NHS checksum, another to perform numerical validation using the final digit, a third to require the presence of an NHS-related keyword, and a fourth to require the presence of a UK-related keyword.

Table 34-165 UK National Health Service (NHS) Number narrow breadth validators

Mandatory validator	Description
UK NHS	UK NHS checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.
Find keywords: NHS-related	At least one of the following keywords or key phrases must be present for the data to match:  national health service, NHS

UK National Health Service (NHS) Number narrow breadth validators Table 34-165 (continued)

Mandatory validator	Description
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:
	uk, united kingdom, britain, england, gb

# UK National Insurance Number data identifier

The UK National Insurance Number is issued by the United Kingdom Department for Work and Pensions (DWP) to identify an individual for the national insurance program. It is also known as a NI number, NINO or NINo.

The UK National Insurance Number data identifier detects the presence of the UK National Insurance Number.

This data identifier provides three breadths of validation:

- Wide See "UK National Insurance Number wide breadth" on page 779.
- Medium See "UK National Insurance Number medium breadth" on page 779.
- Narrow See "UK National Insurance Number narrow breadth" on page 780.

#### UK National Insurance Number wide breadth

The wide breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces, periods, dashes, or together in a string.

The first and second letter cannot be D. F. I. Q. U and V. The second letter also cannot be O.

Table 34-166 UK National Insurance Number wide breadth patterns

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z].\d{2}.\d{2}.\d{2}-[ABCD]	Separated by periods.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not separated.

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separated by spaces.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]-\d{2}-\d{2}-\d{2}-[ABCD]	Separated by dashes.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Digits in a string.

Table 34-166 UK National Insurance Number wide breadth patterns (continued)

### UK National Insurance Number medium breadth

The medium breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces or together in a string.

The first and second letter cannot be D, F, I, Q, U and V; the second letter cannot be O.

Table 34-167 UK National Insurance Number medium breadth patterns

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not delimited.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separated by spaces.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Characters in a string.

## UK National Insurance Number narrow breadth

The narrow breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces or together in a string.

The first and second letter cannot be D, F, I, Q, U and V. The second letter also cannot be O.

UK National Insurance Number narrow breadth patterns Table 34-168

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not delimited.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separated by spaces.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Characters in a string.

The narrow breadth edition of the UK National Insurance Number data identifier implements a validator that requires the presence of a national insurance-related keyword.

Table 34-169 UK National Insurance Number narrow breadth validator

Mandatory validator	Description
Find keywords: Insurance-related	At least one of the following keywords or key phrases must be present for the data to match:
	insurance no., insurance number, insurance#, insurancenumber, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

#### UK National Insurance Number wide breadth

The wide breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces, periods, dashes, or together in a string.

The first and second letter cannot be D, F, I, Q, U and V. The second letter also cannot be O.

UK National Insurance Number wide breadth patterns Table 34-170

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z].\d{2}.\d{2}.\d{2}-[ABCD]	Separated by periods.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not separated.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separated by spaces.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]-\d{2}-\d{2}-\d{2}-[ABCD]	Separated by dashes.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Digits in a string.

### UK National Insurance Number medium breadth

The medium breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces or together in a string.

The first and second letter cannot be D, F, I, Q, U and V; the second letter cannot be O.

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not delimited.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separated by spaces.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Characters in a string.

Table 34-171 UK National Insurance Number medium breadth patterns

#### UK National Insurance Number narrow breadth

The narrow breadth edition of the UK National Insurance Number data identifier implements patterns to detect 9-digit numbers of the format LL DD DD DD L (where L is a letter and D is a digit), separated by spaces or together in a string.

The first and second letter cannot be D, F, I, Q, U and V. The second letter also cannot be O.

Table 34-172 UK National Insurance Number narrow breadth patterns

Pattern	Description
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z]\d{2}\d{2}\d{2}[ABCD]	Not delimited.
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} \d{2} [ABCD] Separated by spaces.	
[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Characters in a string.

The narrow breadth edition of the UK National Insurance Number data identifier implements a validator that requires the presence of a national insurance-related keyword.

UK National Insurance Number narrow breadth validator Table 34-173

Mandatory validator	Description
Find keywords: Insurance-related	At least one of the following keywords or key phrases must be present for the data to match:
	insurance no., insurance number, insurance#, insurancenumber, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

# **UK Passport Number data identifier**

The UK Passport Number identifies a United Kingdom passport using the current official specification of the UK Government Standards of the UK Cabinet Office.

The UK Passport Number data identifier detects the presence of the UK Passport Number.

This data identifier provides three breadths of validation:

- Wide See "UK Passport Number wide breadth" on page 783.
- Medium See "UK Passport Number medium breadth" on page 783.
- Narrow See "UK Passport Number narrow breadth" on page 784.

### **UK Passport Number wide breadth**

The wide breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

Note: The wide breadth edition of the UK Passport Number data identifier does not include any validators.

Table 34-174 UK Passport Number wide breadth pattern

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

## **UK Passport Number medium breadth**

The medium breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

Table 34-175 UK Passport Number medium breadth pattern

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

The medium breadth edition of the UK Passport Number data identifier implements three validators: one to eliminate common test numbers, such as 123456789;

another to eliminate numbers with all the same digits; and a third that requires the presence of a passport-related keyword.

Table 34-176 UK Passport Number medium breadth validators

Mandatory validator	Description	
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 123456789	
Duplicate digits	Ensures that a string of digits are not all the same.	
Find keywords: Passport-related	At least one of the following keywords or key phrases must be present for the data to match:  passport, passport#, passportID, passportno, passportnumber	

# UK Passport Number narrow breadth

The narrow breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

UK Passport Number narrow breadth pattern Table 34-177

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

The narrow breadth edition of the UK Passport Number data identifier implements four validators: one to eliminate common test numbers, such as 123456789; another to eliminate numbers with all the same digits; a third that requires the presence of a passport-related keyword; and a fourth that requires the presence of a UK-related keyword.

UK Passport Number narrow breadth validators Table 34-178

Mandatory validator	Description	
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 123456789	
Duplicate digits	Ensures that a string of digits are not all the same.	
Find keywords: Passport-related	At least one of the following keywords or key phrases must be present for data to match:	
	passport, passport#, passportID, passportno, passportnumber	

ators (continued)
2

Mandatory validator	Description
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:
	uk, united kingdom, britain, england, gb

# UK Passport Number wide breadth

The wide breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

Note: The wide breadth edition of the UK Passport Number data identifier does not include any validators.

UK Passport Number wide breadth pattern Table 34-179

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

## **UK Passport Number medium breadth**

The medium breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

Table 34-180 UK Passport Number medium breadth pattern

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

The medium breadth edition of the UK Passport Number data identifier implements three validators: one to eliminate common test numbers, such as 123456789; another to eliminate numbers with all the same digits; and a third that requires the presence of a passport-related keyword.

UK Passport Number medium breadth validators Table 34-181

Mandatory validator	Description	
Exclude beginning characters	Data beginning with any of the following list of values will not be matched:	
	123456789	

Mandatory validator	Description	
Duplicate digits	Ensures that a string of digits are not all the same.	
Find keywords: Passport-related	At least one of the following keywords or key phrases must be present for the data to match:	
	passport, passport#, passportID, passportno, passportnumber	

Table 34-181 UK Passport Number medium breadth validators (continued)

# UK Passport Number narrow breadth

The narrow breadth edition of the UK Passport Number data identifier implements a pattern to detect 9-digit numbers.

Table 34-182 UK Passport Number narrow breadth pattern

Pattern	Description
\d{9}	Pattern for detecting 9-digit numbers.

The narrow breadth edition of the UK Passport Number data identifier implements four validators: one to eliminate common test numbers, such as 123456789; another to eliminate numbers with all the same digits; a third that requires the presence of a passport-related keyword; and a fourth that requires the presence of a UK-related keyword.

Table 34-183 UK Passport Number narrow breadth validators

Mandatory validator	Description	
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 123456789	
Duplicate digits	Ensures that a string of digits are not all the same.	
Find keywords: Passport-related	At least one of the following keywords or key phrases must be present for the data to match:	
	passport, passport#, passportID, passportno, passportnumber	
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:	
	uk, united kingdom, britain, england, gb	

### **UK Tax ID Number data identifier**

The UK Tax ID Number is a personal identification number provided by the UK Government Standards of the UK Cabinet Office.

The UK Tax ID Number data identifier detects the presence of the UK Tax ID numbers.

This data identifier provides three breadths of validation:

- Wide See "UK Tax ID Number wide breadth" on page 787.
- Medium See "UK Tax ID Number medium breadth" on page 787.
- Narrow See "UK Tax ID Number narrow breadth" on page 787.

#### UK Tax ID Number wide breadth

The wide breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

Note: The wide breadth edition of the UK Tax ID Number data identifier does not include any validators.

Table 34-184	UK Passport Numb	er wide breadth pattern

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

# UK Tax ID Number medium breadth

The medium breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

Table 34-185 UK Tax ID Number medium breadth pattern

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

The medium breadth edition of the UK Tax ID Number data identifier implements two validators: one to eliminates common test numbers, such as 1234567890, and another to eliminate numbers with all the same digit.

Table 34-186 UK Tax ID Number medium breadth validators

Mandatory validator	Description
Duplicate digits	Ensures that a string of digits are not all the same.
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 0123456789, 1234567890, 9876543210, 0987654321

#### UK Tax ID Number narrow breadth

The narrow breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

Table 34-187 UK Tax ID Number narrow breadth pattern

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

The narrow breadth edition of the UK Tax ID Number data identifier implements three validators: one to eliminates common test numbers, such as 1234567890; another to eliminate numbers with all the same digit; and a third that requires the presence of a tax identification-related keyword.

UK Tax ID Number narrow breadth validators Table 34-188

Mandatory validator	Description
Duplicate digits	Ensures that a string of digits are not all the same.
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 0123456789, 1234567890, 9876543210, 0987654321
Find keywords: Tax ID-related	At least one of the following keywords or key phrases must be present for the data to match:  tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax#, taxid#

#### UK Tax ID Number wide breadth

The wide breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

Note: The wide breadth edition of the UK Tax ID Number data identifier does not include any validators.

UK Passport Number wide breadth pattern Table 34-189

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

#### UK Tax ID Number medium breadth

The medium breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

UK Tax ID Number medium breadth pattern Table 34-190

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

The medium breadth edition of the UK Tax ID Number data identifier implements two validators: one to eliminates common test numbers, such as 1234567890, and another to eliminate numbers with all the same digit.

UK Tax ID Number medium breadth validators Table 34-191

Mandatory validator	Description
Duplicate digits	Ensures that a string of digits are not all the same.
Exclude beginning characters	Data beginning with any of the following list of values will not be matched:
	0123456789, 1234567890, 9876543210, 0987654321

#### UK Tax ID Number narrow breadth

The narrow breadth edition of the UK Tax ID Number data identifier implements a single pattern to detect 10-digit numbers.

Table 34-192 UK Tax ID Number narrow breadth pattern

Pattern	Description
\d{10}	Pattern for detecting 10-digit numbers.

The narrow breadth edition of the UK Tax ID Number data identifier implements three validators: one to eliminates common test numbers, such as 1234567890; another to eliminate numbers with all the same digit; and a third that requires the presence of a tax identification-related keyword.

UK Tax ID Number narrow breadth validators Table 34-193

Mandatory validator	Description
Duplicate digits	Ensures that a string of digits are not all the same.
Exclude beginning characters	Data beginning with any of the following list of values will not be matched: 0123456789, 1234567890, 9876543210, 0987654321
Find keywords: Tax ID-related	At least one of the following keywords or key phrases must be present for the data to match:  tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax#, taxid#

# **US Individual Tax Identification Number (ITIN) data** identifier

The US Individual Tax Identification Number (ITIN) is used for tax processing and is issued by the United States Internal Revenue Service (IRS). The IRS issues ITINs to track individuals who are not eligible to obtain Social Security Numbers (SSNs).

The US Individual Tax Identification Number (ITIN) data identifier detects the presence of US ITIN numbers.

This data identifier provides three breadths of validation:

- Wide See "US Individual Tax Identification Number (ITIN) wide breadth" on page 791.
- Medium See "US Individual Tax Identification Number (ITIN) medium breadth" on page 791.

Narrow See "US Individual Tax Identification Number (ITIN) narrow breadth" on page 792.

### US Individual Tax Identification Number (ITIN) wide breadth

The wide breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Note: The wide breadth edition of the US Individual Tax Identification Number (ITIN) data identifier does not include any validators.

Table 34-194 US Individual Tax Identification Number (ITIN) wide breadth patterns

Pattern	Description
9\\d{2}[78]\\d\\d{4}	Pattern for detecting the ITIN format without separators.
9\\d{2}\\\\[78]\\d\\\\\d{4}	Pattern for detecting the ITIN format without separators.
9\d{2}/[78]\d\d{4}	Pattern for detecting the ITIN format separated by slashes.
9\d{2}.[78]\d.\d{4}	Pattern for detecting the ITIN format separated by periods.
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

# US Individual Tax Identification Number (ITIN) medium breadth

The medium breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DDDD separated with dashes, spaces, or periods.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Table 34-195 US Individual Tax Identification Number (ITIN) medium breadth patterns

Pattern	Description
9\d{2}.[78]\d.\d{4}	Pattern for detecting the ITIN format separated by periods.
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.

Table 34-195 US Individual Tax Identification Number (ITIN) medium breadth patterns (continued)

Pattern	Description
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

The medium breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements a single validator to check the surrounding characters.

Table 34-196 US Individual Tax Identification Number (ITIN) medium breadth validator

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.

# US Individual Tax Identification Number (ITIN) narrow breadth

The narrow breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Table 34-197 US Individual Tax Identification Number (ITIN) narrow breadth patterns

Pattern	Description
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

The narrow breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements three validators: one to check the surrounding characters, another to ensure that the digits in the ITIN string are not all the same, and a third that requires the presence of a ITIN-related keyword.

US Individual Tax Identification Number (ITIN) narrow breadth Table 34-198 validators

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Duplicate digits	Ensures that a string of digits are not all the same.

US Individual Tax Identification Number (ITIN) narrow breadth Table 34-198 validators (continued)

Mandatory validator	Description
Find keywords: ITIN-related	At least one of the following keywords or key phrases must be present for the data to be matched.  individual taxpayer identification number, itin, i.t.i.n.

# US Individual Tax Identification Number (ITIN) wide breadth

The wide breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Note: The wide breadth edition of the US Individual Tax Identification Number (ITIN) data identifier does not include any validators.

**Table 34-199** US Individual Tax Identification Number (ITIN) wide breadth patterns

Pattern	Description
9\\d{2}[78]\\d\\d{4}	Pattern for detecting the ITIN format without separators.
9\\d{2}\\\\[78]\\d\\\\\d{4}	Pattern for detecting the ITIN format without separators.
9\d{2}/[78]\d\d{4}	Pattern for detecting the ITIN format separated by slashes.
9\d{2}.[78]\d.\d{4}	Pattern for detecting the ITIN format separated by periods.
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

### US Individual Tax Identification Number (ITIN) medium breadth

The medium breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DDDD separated with dashes, spaces, or periods.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Table 34-200	US Individual Tax Identification Number (ITIN) medium breadth
	patterns

Pattern	Description
9\d{2}.[78]\d.\d{4}	Pattern for detecting the ITIN format separated by periods.
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

The medium breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements a single validator to check the surrounding characters.

US Individual Tax Identification Number (ITIN) medium breadth Table 34-201 validator

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.

# US Individual Tax Identification Number (ITIN) narrow breadth

The narrow breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Table 34-202 US Individual Tax Identification Number (ITIN) narrow breadth patterns

Pattern	Description
9\d{2} [78]\d \d{4}	Pattern for detecting the ITIN format separated by spaces.
9\d{2}-[78]\d-\d{4}	Pattern for detecting the ITIN format separated by dashes.

The narrow breadth edition of the US Individual Tax Identification Number (ITIN) data identifier implements three validators: one to check the surrounding characters, another to ensure that the digits in the ITIN string are not all the same, and a third that requires the presence of a ITIN-related keyword.

Mandatory validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Duplicate digits	Ensures that a string of digits are not all the same.
Find keywords: ITIN-related	At least one of the following keywords or key phrases must be present for the data to be matched.
	individual taxpayer identification number, itin, i.t.i.n.

US Individual Tax Identification Number (ITIN) narrow breadth Table 34-203 validators

### **US Social Security Number (SSN) data identifier**

Note: Starting with Symantec Data Loss Prevention version 12.5, the US Social Security Number (SSN) data identifier is replaced by the Randomized US Social Security Number (SSN) data identifier. Policy templates that use the US SSN data identifier are updated to use the Randomized US SSN data identifier. Symantec recommends that you update your SSN policies to use the Randomized US SSN data identifier. See "Randomized US Social Security Number (SSN) data identifier" on page 759.

The US Individual Tax Identification Number (ITIN) is a personal identification number issued by the Social Security Administration of the United States government. Although primarily used for administering the Social Security program, it is widely used as a personal identification number in many purposes.

The US Social Security Number (SSN) data identifier detects the presence of US Social Security numbers.

This data identifier provides three breadths of validation:

- Wide See "US Social Security Number (SSN) wide breadth" on page 796.
- Medium See "US Social Security Number (SSN) medium breadth" on page 797.
- Narrow See "US Social Security Number (SSN) narrow breadth" on page 798.

### US Social Security Number (SSN) wide breadth

The wide breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Table 34-204 Social Security Number (SSN) wide breadth patterns

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3}.\d{2}.\d{4}	Matches the SSN format delimited by periods.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.
\d{3}\\\d{2}\\\d{4}	Matches the SSN format delimited by backslashes.
\d{3}/\d{2}/\d{4}	Matches the SSN format delimited by forward slashes.
\d{9}	Matches any 9-digit number that is not delimited.

The wide breadth edition of the US Social Security Number (SSN) data identifier implements three validators to ensure that the detected SSN is within validly assigned number ranges, eliminate common test numbers, such as 123456789, and all the same digit.

Social Security Number (SSN) wide breadth validators Table 34-205

Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.

### US Social Security Number (SSN) medium breadth

The medium breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DDDDD separated with dashes, spaces, or periods.

Social Security Number (SSN) medium breadth patterns Table 34-206

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3}.\d{2}.\d{4}	Matches the SSN format delimited by periods.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.

The medium breadth edition of the US Social Security Number (SSN) data identifier implements three validators to ensure that the detected SSN is within validly assigned number ranges, is not a common test number (such as 123456789), and is not all the same digit

Table 34-207 Social Security Number (SSN) medium breadth validators

Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.

### US Social Security Number (SSN) narrow breadth

The narrow breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators.

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.
\d{9}	Matches any 9-digit number not delimited.

Table 34-208 US Social Security Number (SSN) narrow breadth patterns

The narrow breadth edition of the US Social Security Number (SSN) data identifier implements four validators to ensure that the detected SSN is within validly assigned number ranges, is not a common test number (such as 123456789), is not all the same digit, and the message containing the SSN includes a keyword

Social Security Number (SSN) narrow breadth validators Table 34-209

Mandatory Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.
Find keywords: Social security-related	At least one of the following keywords or key phrases must be present for the data to be matched:
	social security number, ssn, ss#

### US Social Security Number (SSN) wide breadth

The wide breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DDDDD separated with dashes, spaces, periods, slashes, or without separators.

The number must begin with a 9 and have a 7 or 8 as the fourth digit.

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3}.\d{2}.\d{4}	Matches the SSN format delimited by periods.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.
\d{3}\\\d{2}\\\d{4}	Matches the SSN format delimited by backslashes.
\d{3}/\d{2}/\d{4}	Matches the SSN format delimited by forward slashes.
\d{9}	Matches any 9-digit number that is not delimited.

Table 34-210 Social Security Number (SSN) wide breadth patterns

The wide breadth edition of the US Social Security Number (SSN) data identifier implements three validators to ensure that the detected SSN is within validly assigned number ranges, eliminate common test numbers, such as 123456789, and all the same digit.

Table 34-211 Social Security Number (SSN) wide breadth validators

Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.

### US Social Security Number (SSN) medium breadth

The medium breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods.

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3}.\d{2}.\d{4}	Matches the SSN format delimited by periods.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.

Table 34-212 Social Security Number (SSN) medium breadth patterns

The medium breadth edition of the US Social Security Number (SSN) data identifier implements three validators to ensure that the detected SSN is within validly assigned number ranges, is not a common test number (such as 123456789), and is not all the same digit

**Table 34-213** Social Security Number (SSN) medium breadth validators

Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.

### US Social Security Number (SSN) narrow breadth

The narrow breadth edition of the US Social Security Number (SSN) data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DDDDD separated with dashes or spaces or without separators.

Table 34-214 US Social Security Number (SSN) narrow breadth patterns

Pattern	Description
\d{3}-\d{2}-\d{4}	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
\d{3} \d{2} \d{4}	Matches the SSN format delimited by spaces.
\d{9}	Matches any 9-digit number not delimited.

The narrow breadth edition of the US Social Security Number (SSN) data identifier implements four validators to ensure that the detected SSN is within validly assigned number ranges, is not a common test number (such as 123456789), is not all the same digit, and the message containing the SSN includes a keyword

Social Security Number (SSN) narrow breadth validators Table 34-215

Mandatory Validator	Description
Number Delimiter	Validates a match by checking the surrounding characters.
Advanced SSN	Checks whether SSN contains zeros in any group, the area number (first group) is less than 773 and not 666, the delimiter between the groups is the same, the number does not consist of all the same digits, and the number is not reserved for advertising (123-45-6789, 987-65-432x).
SSN Area-Group number	For a given area number (first group), not all group numbers (second group) might have been assigned by the SSA. Validator eliminates SSNs with invalid group numbers.
Find keywords: Social security-related	At least one of the following keywords or key phrases must be present for the data to be matched:
	social security number, ssn, ss#

# Chapter

# Library of policy templates

#### This chapter includes the following topics:

- Caldicott Report policy template
- Canadian Social Insurance Numbers policy template
- CAN-SPAM Act policy template
- Common Spyware Upload Sites policy template
- Competitor Communications policy template
- Confidential Documents policy template
- Credit Card Numbers policy template
- Customer Data Protection policy template
- Data Protection Act 1998 (UK) policy template
- Data Protection Directives (EU) policy template
- Defense Message System (DMS) GENSER Classification policy template
- Design Documents policy template
- Employee Data Protection policy template
- Encrypted Data policy template
- Export Administration Regulations (EAR) policy template
- FACTA 2003 (Red Flag Rules) policy template
- Financial Information policy template
- Forbidden Websites policy template

- Gambling policy template
- Gramm-Leach-Bliley policy template
- HIPAA and HITECH (including PHI) policy template
- Human Rights Act 1998 policy template
- Illegal Drugs policy template
- Individual Taxpayer Identification Numbers (ITIN) policy template
- International Traffic in Arms Regulations (ITAR) policy template
- Media Files policy template
- Merger and Acquisition Agreements policy template
- NASD Rule 2711 and NYSE Rules 351 and 472 policy template
- NASD Rule 3010 and NYSE Rule 342 policy template
- NERC Security Guidelines for Electric Utilities policy template
- Network Diagrams policy template
- Network Security policy template
- Offensive Language policy template
- Office of Foreign Assets Control (OFAC) policy template
- OMB Memo 06-16 and FIPS 199 Regulations policy template
- Password Files policy template
- Payment Card Industry (PCI) Data Security Standard policy template
- PIPEDA policy template
- Price Information policy template
- Project Data policy template
- Proprietary Media Files policy template
- Publishing Documents policy template
- Racist Language policy template
- Restricted Files policy template
- Restricted Recipients policy template

- Resumes policy template
- Sarbanes-Oxley policy template
- SEC Fair Disclosure Regulation policy template
- Sexually Explicit Language policy template
- Source Code policy template
- State Data Privacy policy template
- SWIFT Codes policy template
- Symantec DLP Awareness and Avoidance policy template
- UK Drivers License Numbers policy template
- UK Electoral Roll Numbers policy template
- UK National Health Service (NHS) Number policy template
- **UK National Insurance Numbers policy template**
- **UK Passport Numbers policy template**
- UK Tax ID Numbers policy template
- US Intelligence Control Markings (CAPCO) and DCID 1/7 policy template
- US Social Security Numbers policy template
- Violence and Weapons policy template
- Webmail policy template
- Yahoo Message Board Activity policy template
- Yahoo and MSN Messengers on Port 80 policy template

### Caldicott Report policy template

The UK Chief Medical Officer commissioned the Caldicott Report (December, 1997) to improve the way the National Health Service handles and protects patient information. The Caldicott Committee reviewed the confidentiality of data throughout the NHS for purposes other than direct care, medical research, or where there is a statutory requirement for information. Its recommendations are now being put into practice throughout the NHS and in the Health Protection Agency.

The Drug, and Disease, and the Treatment keyword lists are updated with recent keywords based on information from the U.S. Federal Drug Administration (FDA) and other sources.

See "Keep the keyword lists for your HIPAA and Caldicott policies up to date" on page 596.

Caldicott Report policy template rules Table 35-1

Rule	Туре	Description
Patient Data and Drug Keywords		
		<ul> <li>Account number</li> <li>Email</li> <li>ID card number</li> <li>Last name</li> <li>Phone</li> <li>UK NHS (National Health Service) number</li> <li>UK NIN (National Insurance Number)</li> </ul>
Patient Data and Disease Keywords	Compound EDM and Keyword Rule	This compound rule looks for a match among the following EDM data fields in combination with a keyword from the "Disease Names" dictionary. Both conditions must be satisfied for the rule to trigger an incident.  Account number Email ID card number Last name Phone UK NHS (National Health Service) number UK NIN (National Insurance Number)

Rule	Туре	Description	
Patient Data and Treatment Keywords	Compound EDM and Keyword Rule	This compound rule looks for a match among the following EDM dat fields in combination with a keyword from the "Medical Treatment Keywords" dictionary. Both conditions must be satisfied for the rule to trigger an incident:  Account number  Email  ID card number  Last name  Phone  UK NHS (National Health Service) number  UK NIN (National Insurance Number)	
UK NHS Number and Drug Keywords	Simple DCM Rule	This rule looks for a keyword from "UK NIN Keywords" dictionary in combination with a pattern matching the UK NIN data identifier and a keyword from the "Prescription Drug Names" dictionary.	
UK NHS Number and Disease Keywords	Simple DCM Rule	This rule looks for a keyword from "UK NIN Keywords" dictionary in combination with a pattern matching the UK NIN data identifier and a keyword from the "Disease Names" dictionary.	
UK NHS Number and Treatment Keywords	Simple DCM Rule	This rule looks for a keyword from "UK NIN Keywords" dictionary in combination with a pattern matching the UK NIN data identifier and a keyword from the "Medical Treatment Keywords" dictionary.	

**Table 35-1** Caldicott Report policy template rules (continued)

See "Choosing an Exact Data Profile" on page 322.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Canadian Social Insurance Numbers policy template**

This policy detects patterns indicating Canadian social insurance numbers (SINs) at risk of exposure.

DCM Rule **Canadian Social Insurance Numbers** This rule looks for a match to the Canadian Social Insurance Number data identifier and a keyword from the "Canadian Social Ins. No. Words" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **CAN-SPAM Act policy template**

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) establishes requirements for those who send commercial email.

The CAN-SPAM Act template detects activity from an organization's bulk mailer to help ensure compliance with the CAN-SPAM Act requirements.

The detection exception Exclude emails that contain the mandated keywords allows messages to pass that have one or more keywords from the user-defined "CAN-SPAM Exception Keywords" dictionary.

Detection exception: Exclude emails that contain the mandated **Table 35-2** kevwords

Method	Condition	Configuration
Simple exception	Content Matches Keyword (DCM)	<ul> <li>Exclude emails that contain the mandated keywords (Keyword Match):</li> <li>Match keyword from "[physical postal address]" or "advertisement".</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> <li>Note: After you define the keywords, you can choose to count all matches and require 2 keywords from the list to be matched.</li> </ul>

The detection exception CAN-SPAM Compliant Emails excludes from detection document content from the selected IDM index with at least 100% match.

**Table 35-3** Detection exception: CAN-SPAM Compliant Emails

Method	Condition	Configuration
Simple exception	Content Matches Document Profile (IDM)	<ul> <li>Exception for CAN-SPAM compliant emails (IDM):</li> <li>Exact content match (100%)</li> <li>Look in the message body and attachments.</li> <li>Check for existence.</li> <li>See "Choosing an Indexed Document Profile" on page 323.</li> </ul>

If an exception is not met, the detection rule Monitor Email From Bulk Mailer looks for a sender's email address that matches one from the "Bulk Mailer Email Address" list, which is user-defined.

Method	Condition	Configuration
Simple rule	Sender/User Matches Pattern (DCM)	Monitor Email From Bulk Mailer (Sender):  Match sender pattern(s): [bulk-mailer@company.com] (user defined)  Severity: High.

**Table 35-4** Detection rule: Monitor Email From Bulk Mailer

See "Creating a policy from a template" on page 312.

See "Exporting policy detection as a template" on page 350.

### Common Spyware Upload Sites policy template

The Common Spyware Upload Sites policy detects access to common spyware upload Web sites.

DCM Rule	Forbidden Websites 1
	This is a compound rule that looks for either specified IP addresses or URLs in the "Forbidden Websites 1" dictionary.
DCM Rule	Faultiddau Waltata O
DCIVI Rule	Forbidden Websites 2

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Competitor Communications policy template**

The Competitor Communications policy detects forbidden communications with competitors.

DCM Rule	Competitor List
	This rule looks for keywords (domains) from the "Competitor Domains"
	dictionary, which is user-defined.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# **Confidential Documents policy template**

This policy detects company-confidential documents at risk of exposure.

Rules comprising the Confidential Documents template **Table 35-5** 

_					
Rule	Туре	Description			
Confidential Documents, Indexed	Simple IDM Rule with one condition	This rule looks for content from specific documents registered as confidential; returns a match if 80% or more of the source document is found. If you do not have an Indexed Document Profile configured this rule is dropped.			
Confidential Documents	Compound DCM Rule: Attachment/File Type and Keyword Match. Both conditions must match for the rule to trigger an incident.	This rule looks for a combination of keywords from the "Confidential Keywords" list and the following file types:  Microsoft Excel Macro Microsoft Excel Microsoft Works Spreadsheet SYLK Spreadshet Corel Quattro Pro Multiplan Spreadsheet Comma Separate Values Applix Spreadsheets Lotus 1-2-3 Microsoft Word Adobe PDF Microsoft PowerPoint			
Proprietary Documents	Compound DCM Rule: Attachment/File Type and Keyword Match	This compound rule looks for a combination of keywords from the "Proprietary Keywords" dictionary and the above referenced file types.			
Internal Use Only Documents	Compound DCM Rule: Attachment/File Type and Keyword Match	This compound rule looks for a combination of keywords from the "Internal Use Only Keywords" dictionary and the above referenced file types.			
Documents Not For Distribution	Compound DCM Rule: Attachment/File Type and Keyword Match	This compound rule looks for a combination of keywords from the "Not For Distribution Words" dictionary and the above referenced file types.			

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **Credit Card Numbers policy template**

This policy detects patterns indicating credit card numbers at risk of exposure.

DCM Rule Credit Card Numbers, All

> This rule looks for a match to the credit card number system pattern and a keyword from the "Credit Card Number Keywords" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **Customer Data Protection policy template**

This policy detects customer data at risk of exposure.

**Table 35-6** EDM conditions for the Customer Data Protection policy template

Rule name	Туре	Description	Details
Username/Password Combinations	EDM Rule	This rule looks for usernames and passwords in combination with three or more of the following fields:  SSN Phone Email First Name Last Name Bank Card number Account Number ABA Routing Number Canadian Social Insurance Number UK National Insurance Number	However, the following combinations are not a violation:  Phone, email, and last name Email, first name, and last name Phone, first name, and last name

**Table 35-6** EDM conditions for the Customer Data Protection policy template (continued)

Rule name	Туре	Description	Details
Date of Birth	EDM Rule	This rule looks for any three of the following data fields in combination:  SSN Phone Email First Name Last Name Bank Card number Account Number ABA Routing Number Canadian Social Insurance Number UK National Insurance Number Date of Birth	However, the following combinations are not a violation:  Phone, email, and first name Phone, email, and last name Email, first name, and last name Phone, first name, and last name
Exact SSN or CCN	EDM Rule	This rule looks for an exact social security number or bank card number.	
Customer Directory	EDM Rule	This rule looks for Phone or Email.	

DCM conditions for the Customer Data Protection policy template **Table 35-7** 

Rule name	Туре	Description	Details
US Social Security Number Patterns	Compound DCM Rule	This rule looks for a match to the Randomized US Social Security number data identifier and a keyword from the "US SSN Keywords" dictionary.	See "Randomized US Social Security Number (SSN) data identifier" on page 759.
Credit Card Numbers, All	Compound DCM Rule	This rule looks for a match to the credit card number system pattern and a keyword from the "Credit Card Number Keywords" dictionary.	See "Credit Card Number data identifier" on page 715.
ABA Routing Numbers	Compound DCM Rule	This rule looks for a match to the ABA Routing number data identifier and a keyword from the "ABA Routing Number Keywords" dictionary.	See "ABA Routing Number data identifier" on page 702.

See "About the Exact Data Profile and index" on page 371.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Data Protection Act 1998 (UK) policy template

The Data Protection Act 1998 (replacement of Data Protection Act 1984) set standards which must be satisfied when obtaining, holding, using, or disposing of personal data in the UK. The Data Protection Act 1998 covers anything with personal identifiable information (such as data about personal health, employment, occupational health, finance, suppliers, and contractors).

**Table 35-8** UK Data Protection Act. Personal Data detection rule

#### Description

This EDM rule looks for three of the following columns of data:

- NIN (National Insurance Number)
- Account number
- Pin
- Bank card number
- First name
- Last name
- Drivers license
- Password
- Tax payer ID
- UK NHS number
- Date of birth
- Mother's maiden name
- Email address
- Phone number

However, the following combinations are not an incident:

- First name, last name, pin
- First name, last name, password
- First name, last name, email
- First name, last name, phone
- First name, last name, mother's maiden name

**Table 35-9** Additional detection rules in the Data Protection Act 1998 policy template

#### Description

The UK Electoral Roll Numbers rule implements the UK Electoral Roll Number data identifier.

See "UK Electoral Roll Number data identifier" on page 772.

The UK National Insurance Numbers rule implements the narrow breadth edition of the UK National Insurance Number data identifier.

See "UK National Insurance Number data identifier" on page 777.

**Table 35-9** Additional detection rules in the Data Protection Act 1998 policy template (continued)

#### Description

The UK Tax ID Numbers rule implements the narrow edition of the UK Tax ID Number data identifier.

See "UK Tax ID Number data identifier" on page 785.

The UK Drivers License Numbers rule implements the narrow breadth edition of the UK Driver's License number data identifier.

See "UK Drivers License Number data identifier" on page 768.

The **UK Passport Numbers** rule implements the narrow breadth edition of the UK Passport Number data identifier.

See "UK Passport Number data identifier" on page 781.

The UK NHS Numbers rule implements the narrow breadth edition of the UK National Health Service (NHS) Number data identifier.

See "UK National Health Service (NHS) Number data identifier" on page 773.

See "Choosing an Exact Data Profile" on page 322.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Data Protection Directives (EU) policy template

Directives 95/46/EC of the European Parliament deal with the protection of individuals with regard to the processing and free movement of personal data. This policy detects personal data specific to the EU directives.

Table 35-10

Table 35-10
Description
EU Data Protection Directives
This rule looks for any two of the following data columns:
■ Last Name
Bank Card number
■ Drivers license number
■ Account Number
■ PIN
Medical account number
Medical ID card number
■ User name
■ Password
ABA Routing Number
■ Email
■ Phone
■ Mother's maiden name
However, the following combinations do not create a match:
■ Last name, email
■ Last name, phone
■ Last name, account number
■ Last name, username
EU Data Protection, Contact Info
This rule looks for any two of the following data columns: last name, phone, account number,
username, and email.
Except for email internal to the EU
This rule is an exception if the recipient is within the EU. This covers recipients with any of the country
codes from the "EU Country Codes" dictionary.

See "Choosing an Exact Data Profile" on page 322.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# Defense Message System (DMS) GENSER Classification policy template

The Defense Information Systems Agency has established guidelines for Defense Message System (DMS) General Services (GENSER) message classifications, categories, and markings. These standards specify how to mark classified and sensitive documents according to U.S. standards. These standards also provide interoperability with NATO countries and other U.S. allies.

The GENSER policy template enforces GENSER guidelines by detecting information that is classified as confidential. The template contains four simple (single condition) keyword matching (DCM) detection rules. If any rule condition matches, the policy reports an incident.

The detection rule **Top Secret Information** (Keyword Match) looks for any keywords in the "Top Secret Information" dictionary.

Detection rule: Top Secret Information (Keyword Match) Table 35-11

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Top Secret Information (Keyword Match):  Keyword dictionary: "TOP SECRET//"  Severity: High  Check for existence.  Look in envelope, subject, body, attachments.  Case sensitive.  Match on whole or partial words.

The detection rule **Secret Information** (Keyword Match) looks for any keywords in the "Secret Information" dictionary.

Table 35-12 Detection rule: Secret Information (Keyword Match)

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Secret Information (Keyword Match):  Keyword dictionary: "SECRET//"  Severity: High Check for existence Look in envelope, subject, body, attachments Case sensitive Match on whole or partial words.

The detection rule Classified or Restricted Information (Keyword Match) looks for any keywords in the "Classified or Restricted Information" dictionary.

Table 35-13 Detection rule: Classified or Restricted Information (Keyword Match)

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Classified or Restricted Information (Keyword Match):  Keyword dictionary: "CLASSIFIED//,//RESTRICTED//"  Severity: High Check for existence.  Look in envelope, subject, body, attachments.  Case sensitive.  Match on whole or partial words.

The detection rule Other Sensitive Information looks for any keywords in the "Other Sensitive Information" dictionary.

Table 35-14 Other Sensitive Information detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Other Sensitive Information (Keyword Match):  Keyword dictionary: FOR OFFICIAL USE ONLY, SENSITIVE BUT UNCLASSIFIED,DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION  Severity: High Check for existence. Look in envelope, subject, body, attachments.  Case sensitive.  Match on whole words only.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **Design Documents policy template**

This policy detects various types of design documents, such as CAD/CAM, at risk of exposure.

**IDM Rule Design Documents, Indexed** 

> This rule looks for content from specific design documents registered as proprietary. It returns a match if the engine detects 80% or more of

the source document.

DCM Rule **Design Document Extensions** 

This rule looks for the specified file name extensions found in the

"Design Document Extensions" dictionary.

DCM Rule **Design Documents** 

This rule looks for the following specified file types:

cad\_draw

dwg

Note: Both file types and file name extensions are used because the policy does not detect the true file type for all the required documents.

See "Choosing an Indexed Document Profile" on page 323.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Employee Data Protection policy template**

This policy detects employee data at risk of exposure.

EDM rules for Employee Data Protection **Table 35-15** 

Name	Туре	Description
Username/Password Combinations	EDM Rule	This rule looks for usernames and passwords in combination with any three of the following data fields.  SSN Phone Email First Name Last Name Bank Card Number Account Number ABA Routing Number Canadian Social Insurance Number UK National Insurance Number Date of Birth
Employee Directory	EDM Rule	This rule looks for Phone or Email.

DCM rules for Employee Data Protection **Table 35-16** 

Name	Туре	Description
US Social Security Number Patterns	DCM Rule	This rule looks for a match from the Randomized US Social Security Number (SSN) data identifier and a keyword from the "US SSN Keywords" dictionary.
		See "Randomized US Social Security Number (SSN) data identifier" on page 759.
Credit Card Numbers, All	DCM Rule	This rule looks for a match from the credit card number system pattern and a keyword from the "Credit Card Number Keywords" dictionary.
		See "Credit Card Number data identifier" on page 715.
ABA Routing Numbers	DCM Rule	This rule looks for a match from the ABA Routing number data identifier and a keyword from the "ABA Routing Number Keywords" dictionary.
		See "ABA Routing Number data identifier" on page 702.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Encrypted Data policy template**

This policy detects the use of encryption by a variety of methods including S/MIME, PGP, GPG, and file password protection.

DCM Rule Password Protected Files

This rule looks for the following file types: encrypted zip, encrypted doc,

encrypted xls, or encrypted ppt.

DCM Rule **PGP Files** 

This rule looks for the following file type: pgp.

DCM Rule **GPG Files** 

This rule looks for a keyword from the "GPG Encryption Keywords"

dictionary.

DCM Rule S/MIME

This rule looks for a keyword from the "S/MIME Encryption Keywords"

dictionary.

DCM Rule **HushMail Transmissions** 

This rule looks for a match from a list of recipient URLs.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# Export Administration Regulations (EAR) policy template

The U.S. Department of Commerce enforces the Export Administration Regulations (EAR). These regulations primarily cover technologies and technical information with commercial and military applicability. These technologies are also known as dual-use technologies, for example, chemicals, satellites, software, computers, and so on.

This Export Administration Regulations (EAR) template detects violations from regulated countries and controlled technologies.

The detection rule Indexed EAR Commerce Control List Items and Recipients looks for a country code in the recipient from the "EAR Country Codes" dictionary and for a specific "SKU" from an Exact Data Profile index (EDM). Both conditions must match to trigger an incident.

**Table 35-17** Detection rule: Indexed EAR Commerce Control List Items and Recipients

Method	Condition	Configuration
Compound rule	Content Matches Exact Data (EDM)	See "Choosing an Exact Data Profile" on page 322.
	Content Matches Keyword (DCM)	

The detection rule EAR Commerce Control List and Recipients looks for a country code in the recipient from the "EAR Country Codes" list and a keyword from the "EAR CCL Keywords" dictionary. Both conditions must match to trigger an incident.

Table 35-18 Detection rule: EAR Commerce Control List and Recipients

Method	Condition	Configuration
Compound rule Recipient Matches (DCM)	Recipient Matches Pattern (DCM)	<ul> <li>EAR Commerce Control List and Recipients (Recipient):</li> <li>Match: Email address OR URL domain suffixes.</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>At least 1 recipient(s) must match.</li> <li>Matches on entire message.</li> </ul>
	Content Matches Keyword (DCM)	EAR Commerce Control List and Recipients (Keyword Match):  Match: EAR CCL Keywords  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# FACTA 2003 (Red Flag Rules) policy template

This policy helps to address sections 114 and 315 (or Red Flag Rules) of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. These rules specify that a financial institution or creditor that offers or maintains covered accounts must develop and implement an identity theft prevention program. FACTA is designed

to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

The Username/Password Combinations detection rule detects the presence of both a user name and password from a profiled database index.

Username/Password Combinations detection rule Table 35-19

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	This condition detects exact data containing both of the following data items:
		<ul><li>User name</li><li>Password</li></ul>
		See "Choosing an Exact Data Profile" on page 322.

The **Exact SSN or CCN** detection rule detects the presence of either a social security number or a credit card number from a profiled database.

Table 35-20 Exact SSN or CCN detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	This condition detects exact data containing either of the following data columns:
		<ul><li>Social security number (Taxpayer ID)</li><li>Bank Card Number</li></ul>
		See "Choosing an Exact Data Profile" on page 322.

The Customer Directory detection rule detects the presence of either an email address or a phone number from a profiled database.

Customer Directory detection rule Table 35-21

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	This condition detects exact data containing either of the following data columns:
		<ul> <li>Email address</li> <li>Phone number</li> <li>See "Choosing an Exact Data Profile" on page 322.</li> </ul>

The Three or More Data Columns detection rule detects exact data containing three or more of data items from a profiled database index.

Table 35-22 Three or More Data Columns detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	Detects exact data containing three or more of the following data items:  ABA Routing Number Account Number Bank Card Number Birth Date Email address First Name Last Name National Insurance Number Password Phone Number Social Insurance Number Social security number (Taxpayer ID) User name  However, the following combinations are not a match: Phone Number, Email, First Name Phone Number, First Name, Last Name See "Choosing an Exact Data Profile" on page 322.

The US Social Security Number Patterns detection rule implements the narrow breadth edition of the Randomized US Social Security Number (SSN) system data identifier.

See "Randomized US Social Security Number (SSN) data identifier" on page 759.

This data identifier detects nine-digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators. The number must be in valid assigned number ranges. This condition eliminates common test numbers, such as 123456789 or all the same digit. It also requires the presence of a Social Security keyword.

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul> <li>Data Identifier: Randomized US Social Security Number (SSN) narrow breadth         See "Randomized US Social Security Number (SSN) data identifier" on page 759.</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>

Table 35-23 US Social Security Number Patterns detection rule

The Credit Card Numbers, All detection rule implements the narrow breadth edition of the Credit Card Number system Data Identifier.

See "Credit Card Number data identifier" on page 715.

This data identifier detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. This condition performs Luhn check validation and includes formats for American Express, Diner's Club, Discover, Japan Credit Bureau (JCB), MasterCard, and Visa. It eliminates common test numbers, including those reserved for testing by credit card issuers. It also requires the presence of a credit card keyword.

Credit Card Numbers, All detection rule Table 35-24

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul> <li>Data Identifier: Credit Card Number narrow breadth         See "Credit Card Number narrow breadth" on page 723.</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>

The ABA Routing Numbers detection rule implements the narrow breadth edition of the ABA Routing Number system Data Identifier.

See "ABA Routing Number data identifier" on page 702.

This data identifier detects nine-digit numbers. It validates the number using the final check digit. This condition eliminates common test numbers, such as 123456789, number ranges that are reserved for future use, and all the same digit. This condition also requires the presence of an ABA keyword.

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul> <li>Data Identifier: ABA Routing Number narrow breadth         See "ABA Routing Number narrow breadth" on page 705.</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>

Table 35-25 ABA Routing Numbers detection rule

See "Creating a policy from a template" on page 312.

See "Exporting policy detection as a template" on page 350.

# Financial Information policy template

The Financial Information policy detects financial data and information.

IDM Rule	Financial Information, Indexed	
	This rule looks for content from specific financial information files registered as proprietary; returns a match if 80% or more of the source document is found.	
DCM Rule	Financial Information	
	This rule looks for the combination of specified file types, keywords from the "Financial Keywords" dictionary, and keywords from the "Confidential/Proprietary Words" dictionary.	
	The specified file types are as follows:	
	<ul> <li>excel_macro</li> <li>xls</li> <li>works_spread</li> <li>sylk</li> <li>quattro_pro</li> <li>mod</li> <li>csv</li> <li>applix_spread</li> <li>123</li> </ul>	

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Forbidden Websites policy template

The Forbidden Websites policy template is designed to detect access to specified web sites.

Note: To process HTTP GET requests appropriately, you may need to configure the Network Prevent for Web server. See "To enable a Forbidden Website policy to process GET requests appropriately" on page 823.

Forbidden Websites policy template **Table 35-26** 

DCM Keyword Rule	Description
Forbidden Websites	This rule looks for any keywords in the "Forbidden Websites" dictionary, which is user-defined.

#### To enable a Forbidden Website policy to process GET requests appropriately

- Configure your web proxy server to forward GET requests to the Network Prevent for Web server.
- Set the L7.processGets Advanced Server Setting on the Network Prevent for Web server to "true" (which is the default).
- 3 Reduce the L7.minSizeofGetURL Advanced Server Setting on the Network Prevent for Web server from the default of 100 to a number of bytes (characters) smaller than the length of the shortest web site that the policy specifies

Note: Reducing the minimum size of GETs increases the number of URLs that have to be processed, which increases server traffic load. One approach is to calculate the number of characters in the shortest URL specified in the list of forbidden URLs and set the minimum size to that number. Another approach is to set the minimum URL size to 10 as that should cover all cases.

You may need to adjust the "Ignore Requests Smaller Than" setting in the ICAP configuration of the Network Prevent server from the default 4096 bytes. This value stops processing of incoming web pages that contain fewer bytes than the number specified. If a page of a forbidden web site URL might be smaller than that number, the setting should be reduced appropriately.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **Gambling policy template**

This policy detects any reference to gambling.

Gambling policy template Table 35-27

DCM Keyword Rule	DCM Rule
Suspicious Gambling Keywords	This rule looks for five instances of keywords from the "Gambling Keywords, Confirmed" dictionary.
Less Suspicious Gambling Keywords	This rule looks for ten instances of keywords from the "Gambling Keywords, Suspect" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **Gramm-Leach-Bliley policy template**

The Gramm-Leach-Bliley (GLB) Act gives consumers the right to limit some sharing of their information by financial institutions.

The Gramm-Leach-Bliley policy template detects transmittal of customer data.

**Table 35-28** Gramm-Leach-Bliley policy template conditions

Detection method	Туре	Description
Username/Password Combinations	Simple rule: EDM	This rule looks for user names and passwords in combination.  See "Choosing an Exact Data Profile" on page 322.
Exact SSN or CCN	Simple rule: EDM	This rule looks for SSN or Credit Card Number.
Customer Directory	Simple rule: EDM	This rule looks for Phone or Email.

Gramm-Leach-Bliley policy template conditions (continued) **Table 35-28** 

Detection method	Туре	Description
3 or more critical customer fields	Simple rule: EDM	This rule looks for a match among any three of the following fields:  Account number  Bank card number  Email address  First name  Last name  PIN number  Phone number  Social security number  ABA Routing Number  Canadian Social Insurance Number  UK National Insurance Number  Date of Birth  However, the following combinations are not a match:  Phone, email, and first name  Phone, email, and last name  Email, first name, and last name  Phone, first name, and last name
ABA Routing Numbers	Simple rule: DCM (DI)	This condition detects nine-digit numbers. It validates the number using the final check digit. This condition eliminates common test numbers, such as 123456789, number ranges that are reserved for future use, and all the same digit. This condition also requires the presence of an ABA-related keyword.  See "ABA Routing Number narrow breadth" on page 705.
US Social Security Numbers	Simple rule: DCM (DI)	This rule looks for social security numbers. For this rule to match, there must be a number that fits the Randomized US SSN data identifier. There must also be a keyword or phrase that indicates the presence of a US SSN with a keyword from "US SSN Keywords" dictionary. The keyword condition is included to reduce false positives with any numbers that may match the SSN format.  See "Randomized US Social Security Number (SSN) data identifier" on page 759.

Detection method	Туре	Description
Credit Card Numbers	Simple rule: DCM (DI)	This condition detects valid credit card numbers that are separated by spaces, dashes, periods, or without separators. This condition performs Luhn check validation and includes the following credit card formats:  American Express Diner's Club Discover Japan Credit Bureau (JCB) MasterCard Visa This rule eliminates common test numbers, including those reserved for testing by credit card issuers, and also requires the presence of a credit card-related keyword.  See "Credit Card Number narrow breadth" on page 723.

Table 35-28 Gramm-Leach-Bliley policy template conditions (continued)

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### HIPAA and HITECH (including PHI) policy template

The HIPAA and HITECH (including PHI) policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA). Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for protected health information (PHI).

This policy template detects data concerning prescription drugs, diseases, and treatments in combination with PHI. Organizations that are not subject to HIPAA can also use this policy to control PHI data.

In Symantec Data Loss Prevention version 12.5, the HIPAA and HITECH (including PHI) policy template is updated with recent Drug, and Disease, and Treatment keyword lists based on information from the U.S. Federal Drug Administration (FDA) and other sources. The policy template is also updated to use the Randomized US Social Security Number (SSN) data identifier, which detects both traditional and randomized SSNs.

See "Keep the keyword lists for your HIPAA and Caldicott policies up to date" on page 596.

See "Updating policies to use the Randomized US SSN data identifier" on page 569.

Table 35-29 describes the TPO exception that is provided by the template. TPOs (Treatment, Payment, or health care Operations) are service providers to health care organizations and have an exception for HIPAA information restrictions. The template requires that you enter the allowed email addresses. If implemented the exception is evaluated before detection rules and the policy does not trigger an incident if the protected information is sent to one of the allowed partners.

Table 35-29 TPO exception

Name	Туре	Configuration
TPO Exception	Content Matches Keyword (DCM)	Simple exception (single condition match).  Looks for a recipient email address matching one from the "TPO Email Addresses" user-defined keyword dictionary.

The Table 35-30 looks for a exact data match against any single column from a profiled Patient Data database record.

Patient Data detection rule Table 35-30

Name	Туре	Configuration
Patient Data	Content Matches Exact Data (EDM)	Match data from any single field:  Last name Tax payer ID (SSN) Email address Account number ID card number Phone number See "Choosing an Exact Data Profile" on page 322.

The Table 35-31 is a compound detection rule that requires a Patient Data exact match and a match from the "Drug Code" data identifier.

Name	Condition types	Configuration
Patient Data and Drug Codes	(EDM) And Content Matches Data Identifier	Looks for a match against any single column from a profiled Patient Data database record and a match from the National Drug Code data identifier.  See Table 35-30 on page 827.  See "National Drug Code (NDC) data identifier" on page 754.

Table 35-31 Patient Data and Drug Codes detection rule

The Table 35-32 is a compound detection rule that requires a Patient Data exact match and a keyword match from the "Prescription Drug Names" dictionary.

Patient Data and Prescription Drug Names detection rule Table 35-32

Name	Condition type	Configuration
Patient Data and Prescription Drug Names	Content Matches Exact Data (EDM) AND Content Matches Keyword (DCM)	Looks for a match against any single column from a profiled Patient Data database record and a keyword match from the Prescription Drug Names dictionary See Table 35-30 on page 827.  See "Updating policies after upgrading to the latest version" on page 355.

Table 35-33 is a compound detection rule that requires a Patient Data exact match and keyword match from the "Medical Treatment Keywords" dictionary.

Patient Data and Treatment Keywords detection rule Table 35-33

Name	Condition type	Configuration
Patient Data and Treatment Keywords	Content Matches Exact Data (EDM) And Content Matches Keyword (DCM)	Looks for a match against any single column from a profiled Patient Data database record and a keyword match from the Medical Treatment Keywords dictionary.  See Table 35-30 on page 827.  See "Updating policies after upgrading to the latest version" on page 355.

Table 35-34 is a compound detection rule that requires a Patient Data exact match and a keyword match from the "Disease Names" dictionary.

		,
Name	Condition type	Configuration
Patient Data and Disease Keywords	Content Matches Exact Data (EDM) And Content Matches Keyword	Looks for a match against any single column from a profiled Patient Data database record.and a keyword match from the Disease Names dictionary.  See Table 35-30 on page 827.
	(DCM)	See "Updating policies after upgrading to the latest version" on page 355.

Table 35-34 Patient Data and Disease Keywords detection rule

Table 35-35 is a compound detection rule that looks for SSNs using the Randomized US Social Security Number (SSN) data identifier and for a keyword from the "Prescription Drug Names" dictionary.

**Table 35-35** SSN and Drug Keywords detection rule

Name	Condition type	Configuration
SSN and Drug Keywords	Content Matches Data Identifier	Randomized US Social Security Number (SSN) data identifier (narrow breadth)
	And Content Matches Keyword	See "Randomized US Social Security Number (SSN) data identifier" on page 759.  Prescription Drug Names keyword dictionary
		See "Updating policies after upgrading to the latest version" on page 355.

Table 35-36 is a compound detection rule that looks for SSNs using the Randomized US Social Security Number (SSN) data identifier and for a keyword match from the "Medical Treatment Keywords" dictionary.

SSN and Treatment Keywords detection rule Table 35-36

Name	Condition type	Configuration
SSN and Treatment Keywords	Content Matches Data Identifier	Randomized US Social Security Number (SSN) data identifier (narrow breadth)
	And Content Matches Keyword	See "Randomized US Social Security Number (SSN) data identifier" on page 759.  Medical Treatment Keywords keyword dictionary.  See "Updating policies after upgrading to the latest version" on page 355.

Table 35-37 is a compound detection rule that looks for SSNs using the Randomized US Social Security Number (SSN) data identifier and for a keyword match from the "Disease Names" dictionary.

**Table 35-37** SSN and Disease Keywords detection rule

Name	Condition type	Configuration
SSN and Disease Keywords	Content Matches Data Identifier	Randomized US Social Security Number (SSN) data identifier (narrow breadth)
	And Content Matches Keyword	See "Randomized US Social Security Number (SSN) data identifier" on page 759.  Disease Names keyword dictionary  See "Updating policies after upgrading to the latest version" on page 355.

Table 35-38 is a compound detection rule that looks for SSNs using the Randomized US Social Security Number (SSN) data identifier and for a drug code using the Drug Code data identifier.

SSN and Drug Code detection rule **Table 35-38** 

Name	Condition type	Configuration
SSN and Drug Code	Content Matches Data Identifier	Randomized US Social Security Number (SSN) data identifier (narrow breadth)
	And Content Matches Keyword	See "Randomized US Social Security Number (SSN) data identifier" on page 759.
		Drug Code data identifier (narrow breadth)
		See "National Drug Code (NDC) data identifier" on page 754.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# **Human Rights Act 1998 policy template**

The Human Rights Act 1998 allows UK citizens to assert their rights under the European Convention on Human Rights in UK courts and tribunals. The Act states that "so far as possible to do so, legislation must be read and given effect in a way which is compatible with convention rights." The Human Rights Act 1998 policy enforces Article 8 by ensuring that the private lives of British citizens stay private.

**EDM Rule UK Data Protection Act, Personal Data** 

> This compound rule looks for two data types, last name and electoral roll number, in combination with a keyword from the "UK Personal Data

Keywords" dictionary.

DCM Rule **UK Electoral Roll Numbers** 

This rule looks for a single compound condition with four parts:

- A single keyword from the "UK Keywords" dictionary
- A pattern matching that of the UK Electoral Roll Number data identifier
- A single keyword from the "UK Electoral Roll Number Words" dictionary
- A single keyword from the "UK Personal Data Keywords" dictionary

See "Choosing an Exact Data Profile" on page 322.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Illegal Drugs policy template

This policy detects conversations about illegal drugs and controlled substances.

DCM Rule **Street Drugs** This rule looks for five instances of keywords from the "Street Drug Names" dictionary. DCM Rule Mass Produced Controlled Substances This rule looks for five instances of keywords from the "Manufactured Controlled Substances" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Individual Taxpayer Identification Numbers (ITIN) policy template

An Individual Taxpayer Identification Number (ITIN) is a tax-processing number issued by the US Internal Revenue Service (IRS). The IRS issues ITINs to track individuals are not eligible to obtain Social Security Numbers (SSNs).

DCM Keyword Rule	Description
ITIN	This rule looks for a match to the US ITIN data identifier and a keyword from the "US ITIN Keywords" dictionary.

ITIN policy template conditions

See "Configuring policies" on page 326.

Table 35-39

See "Exporting policy detection as a template" on page 350.

### International Traffic in Arms Regulations (ITAR) policy template

The International Traffic in Arms Regulations (ITAR) are enforced by the US Department of State. Exporters of defense services or related technical data are required to register with the federal government and may need export licenses. This policy detects potential violations based on countries and controlled assets designated by the ITAR.

The Indexed ITAR Munition Items and Recipients detection rule looks for a country code in the recipient from the "ITAR Country Codes" dictionary and for a specific "SKU" from an indexed FDM file.

Table 35-40 Indexed ITAR Munition Items and Recipients detection rule

Method	Conditions (both must match)	Configuration
Compound rule	Recipient Matches Pattern (DCM)	Match recipient email or URL domain from ITAR Country Codes list:  Severity: High. Check for existence. At least 1 recipient(s) must match.
	Content Matches Exact Data (EDM)	See "Choosing an Exact Data Profile" on page 322.

The ITAR Munitions List and Recipients detection rule looks for both a country code in the recipient from the "ITAR Country Codes" dictionary and a keyword from the "ITAR Munition Names" dictionary.

		,
Method	Conditions (both must match)	Configuration
Compound rule	Recipient Matches Pattern (DCM)	Match recipient email or URL domain from ITAR Country Codes list:  Severity: High. Check for existence. At least 1 recipient pattern must match.
	Content Matches Keyword (DCM)	Match any keyword from the ITAR Munitions List:  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only. Severity: High.

Table 35-41 ITAR Munitions List and Recipients detection rule

See "Exporting policy detection as a template" on page 350.

### Media Files policy template

The Media Files policy detects various types of video and audio files (including mp3).

DCM Rule

### **Media Files**

This rule looks for the following media file types:

- qt
- macromedia\_dir
- midi
- mp3
- mpeg\_movie
- quickdraw
- realaudio
- wav
- video win
- vrml

DCM Rule **Media Files Extensions** 

> This rule looks for file name extensions from the "Media Files Extensions" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Merger and Acquisition Agreements policy template

The Mergers and Acquisition Agreements policy template detects contracts and official documentation concerning merger and acquisition activity.

You can modify this template with company-specific code words to detect specific deals.

The Merger and Acquisition Agreements template provides a single compound detection rule. All conditions in the rule must match for the rule to trigger an incident.

Merger and Acquisition Agreements compound detection rule Table 35-42

Condition	Configuration
Contract Specific Keywords (Keyword Match)	<ul> <li>Match any keyword: merger, agreement, contract, letter of intent, term sheet, plan of reorganization</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> </ul>
Acquisition Corporate Structure Keywords (Keyword Match)	<ul> <li>Match any keyword: subsidiary, subsidiaries, affiliate, acquiror, merger sub, covenantor, acquired company, acquiring company, surviving corporation, surviving company</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> </ul>

Table 35-42 Merger and Acquisition Agreements compound detection rule (continued)

Condition	Configuration
Merger Consideration Keywords (Keyword Match)	<ul> <li>Match any keyword: merger stock, merger consideration, exchange shares, capital stock, dissenting shares, capital structure, escrow fund, escrow account, escrow agent, escrow shares, escrow cash, escrow amount, stock consideration, break-up fee, goodwill</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> </ul>
Legal Contract Keywords (Keyword Match)	<ul> <li>Match any keyword: recitals, in witness whereof, governing law, Indemnify, Indemnified, indemnity, signature page, best efforts, gross negligence, willful misconduct, authorized representative, severability, material breach</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> </ul>

See "Exporting policy detection as a template" on page 350.

# NASD Rule 2711 and NYSE Rules 351 and 472 policy template

This policy protects the name(s) of any companies involved in an upcoming stock offering, internal project names for the offering, and the stock ticker symbols for the offering companies.

The NASD Rule 2711 Documents, Indexed detection rule looks for content from specific documents registered as sensitive and known to be subject to NASD Rule 2711 or NYSE Rules 351 and 472. This rule returns a match if 80% or more of the source document is found.

NASD Rule 2711 Documents, Indexed detection rule

Method	Condition	Configuration
Simple rule	Content Matches Document Signature (IDM)	NASD Rule 2711 Documents, Indexed (IDM):  Detect documents in selected Indexed Document Profile Require at least 80% content match. Severity: High. Check for existence. Look in body, attachments.  See "Choosing an Indexed Document Profile" on page 323.

Table 35-43

The NASD Rule 2711 and NYSE Rules 351 and 472 detection rule is a compound rule that contains a sender condition and a keyword condition. The sender condition is based on a user-defined list of email addresses of research analysts at the user's company ("Analysts' Email Addresses" dictionary). The keyword condition looks for any upcoming stock offering, internal project names for the offering, and the stock ticker symbols for the offering companies ("NASD 2711 Keywords" dictionary). Like the sender condition, it requires editing by the user.

NASD Rule 2711 and NYSE Rules 351 and 472 detection rule Table 35-44

Method	Condition	Configuration
Compound rule	Sender/User Matches Pattern (DCM)	NASD Rule 2711 and NYSE Rules 351 and 472 (Sender):  Match sender pattern(s) [research_analyst@company.com] (user defined)  Severity: High.  Matches on entire message.
	Content Matches Keyword (DCM)	NASD Rule 2711 and NYSE Rules 351 and 472 (Keyword Match):  Match "[company stock symbol]", "[name of offering company]", "[offering name (internal name)]".  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### NASD Rule 3010 and NYSE Rule 342 policy template

NASD Rule 3010 and NYSE Rule 342 require brokers-dealers to supervise certain brokerage employees' communications. The NASD Rule 3010 and NYSE Rule 342 policy monitors the communications of registered principals who are subject to these regulations.

The Stock Recommendation detection rule looks for a keyword from the "NASD 3010 Stock Keywords" dictionary and the "NASD 3010 Buy/Sell Keywords" dictionary. In addition, this rule requires evidence of a stock recommendation in combination with a buy or sell action.

Table 35-45 Stock Recommendation detection rule

Method	Conditions (all must match)	Configuration
Compound rule	Content Matches Keyword (DCM)	Match keyword: "recommend"  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.
	Content Matches Keyword (DCM)	Match keyword: "buy" or "sell"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.
Content Matches Keyword (DCM)		Match keyword: "stock, stocks, security, securities, share, shares"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

The NASD Rule 3010 and NYSE Rule 342 Keywords detection rule looks for keywords in the "NASD 3010 General Keywords" dictionary, which look for any general stock broker activity, and stock keywords.

Table 35-46	NASD Rule 3010 and NYSE Rule 342 Keywords detection rule

Method	Conditions (both must match)	Configuration
Compound rule	Content Matches Keyword (DCM)	Match keyword: "authorize", "discretion", "guarantee", "options"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.
	Content Matches Keyword (DCM)	Match keyword: "stock, stocks, security, securities, share, shares"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

See "Exporting policy detection as a template" on page 350.

# **NERC Security Guidelines for Electric Utilities policy** template

The North American Electric Reliability Council (NERC) Guideline for Protecting Potentially Sensitive Information describes how to protect and secure data about critical electricity infrastructure.

This policy detects the information outlined in the NERC security guidelines for the electricity sector.

Key Response Personnel detection rule Table 35-47

Detection method	Match condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	Match any three of the following data items:  First name Last name Phone Email  See "Choosing an Exact Data Profile" on page 322.

Table 35-48	Network	Infrastructure	Maps	detection rule
-------------	---------	----------------	------	----------------

Detection method	Match condition	Configuration
Simple rule	Content Matches Indexed	This rule requires an exact binary match.
	Documents (IDM)	See "Choosing an Indexed Document Profile" on page 323.

The Sensitive Keywords and Vulnerability Keywords detection rule looks for any keyword matches from the "Sensitive Keywords" dictionary and the "Vulnerability Keywords" dictionary.

Table 35-49 Sensitive Keywords and Vulnerability Keywords detection rule

<b>Detection method</b>	Match conditions	Configuration
Compound rule	Content Matches Keyword (DCM)	Match any Sensitive Keyword:  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.
	Content Matches Keyword (DCM)	Match any Vulnerability Keyword:  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Network Diagrams policy template**

The Network Diagrams policy detects computer network diagrams at risk of exposure.

**IDM Rule Network Diagrams, Indexed** 

> This rule looks for content from specific network diagrams that are registered as confidential. This rule returns a match if 80% or more of the source document is detected.

DCM Rule **Network Diagrams with IP Addresses** 

This rule looks for a Visio file type in combination with an IP address

data identifier.

DCM Rule **Network Diagrams with IP Address Keyword** 

This rule looks for a Visio file type in combination with phrase variations

of "IP address" with a data identifier.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Network Security policy template

The Network Security policy detects evidence of hacking tools and attack planning.

DCM Rule GoToMyPC Activity

This rule looks for a GoToMyPC command format with a data identifier.

DCM Rule **Hacker Keywords** 

This rule looks for a keyword from the "Hacker Keywords" dictionary.

DCM Rule **KeyLoggers Keywords** 

This rule looks for a keyword from the "Keylogger Keywords" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Offensive Language policy template

The Offensive Language policy detects the use of offensive language.

DCM Rule Offensive Language, Explicit

This rule looks for any single keyword in the "Offensive Language,

Explicit" dictionary.

DCM Rule Offensive Language, General

This rule looks for any three instances of keywords in the "Offensive

Language, General" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Office of Foreign Assets Control (OFAC) policy template

The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions. These sanctions are based on US foreign policy and national security goals against certain countries, individuals, and organizations. The Office of Foreign Assets Control (OFAC) policy detects communications involving these targeted groups.

The OFAC policy has two primary parts. The first deals with the Specially Designated Nationals (SDN) list, and the second deals with general OFAC policy restrictions.

The SDN list refers to specific people or organizations that are subject to trade restrictions. The U.S. Treasury Department provides text files with specific names, last known addresses, and known aliases for these individuals and entities. The Treasury Department stipulates that the addresses may not be correct or current. and different locations do not change the restrictions on people and organizations.

In the OFAC policy template, Symantec Data Loss Prevention has scrubbed the list to make it more usable and practical. This includes extracting keywords and key phrases from the list of names and aliases, since names do not always appear in the same format as the list. Also, common names have been removed to reduce false positives. For example, one organization on the SDN list is known as "SARA." Leaving this on the list would generate a high false positive rate. "SARA Properties" is another entry on the list. It is used as a key phrase in the template because the incidence of this phrase is much lower than "SARA" alone. The list of names and organizations is considered in combination with the commonly found countries in the SDN address list. The top 12 countries on the list are considered, after again removing more commonly occurring countries. The template looks for recipients with any of the listed countries as the designated country code. This SDN list minimizes false positives while still detecting transactions or communications with known restricted parties.

The OFAC policy also provides guidance around the restrictions the U.S. Treasury Department has placed on general trade with specific countries. This is distinct from the SDN list, since individuals and organizations are not specified. The list of general sanctions can be found here:

http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml

The Office of Foreign Assets Control (OFAC) template looks for recipients on the OFAC- listed countries by designated country code.

The OFAC Special Designated Nationals List and Recipients detection rule looks for a recipient with a country code matching entries in the "OFAC SDN Country Codes" specification in combination with a match on a keyword from the "Specially Designated Nationals List" dictionary.

Table 35-50 OFAC Special Designated Nationals List and Recipients detection

Method	Condition	Configuration
Compound rule	Recipient Matches Pattern (DCM)	OFAC Special Designated Nationals List and Recipients (Recipient):  Match email or URL domain by OFAC SDN Country Code.  Severity: High.  Check for existence.  At least 1 recipient(s) must match.  Matches on the entire message.
	Content Matches Keyword (DCM)	Specially Designated Nationals List (Keyword Match):  Match keyword from the Specially Designated Nationals List.  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

The Communications to OFAC countries detection rule looks for a recipient with a country code matching entries from the "OFAC Country Codes" list.

Table 35-51 Communications to OFAC countries detection rule

Method	Condition	Configuration
Simple rule	Recipient Matches Pattern (DCM)	Communications to OFAC countries (Recipient):  Match email or URL domain by OFAC Country Code.  Severity: High.  Check for existence.  At least 1 recipient(s) must match.
		■ Matches on the entire message.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### OMB Memo 06-16 and FIPS 199 Regulations policy template

This policy detects information classified as confidential according to the guidelines established in the Federal Information Processing Standards (FIPS) Publication 199 from the National Institute of Standards and Technology (NIST). NIST is responsible for establishing standards and guidelines for data security under the Federal Information Security Management Act (FISMA).

This template contains three simple detection rules. If any rule reports a match, the policy triggers an incident.

The High Confidentiality Indicators detection rule looks for any keywords in the "High Confidentiality" dictionary.

**Table 35-52** High Confidentiality Indicators detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword	High Confidentiality Indicators (Keyword Match):  Match "(confidentiality, high)", "(confidentiality,high)"  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

The Moderate Confidentiality Indicators detection rule looks for any keywords in the "Moderate Confidentiality" dictionary.

Table 35-53 Moderate Confidentiality Indicators detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword	Moderate Confidentiality Indicators (Keyword Match):  Match "(confidentiality, moderate)", "(confidentiality,moderate)"  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

The Low Confidentiality Indicators detection rule looks for any keywords in the "Low Confidentiality" dictionary.

Method	Condition	Configuration
Simple rule	Content Matches Keyword	Low Confidentiality Indicators (Keyword Match):  Match "(confidentiality, low)", "(confidentiality,low)"  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.

Table 35-54 Low Confidentiality Indicators detection rule

See "Exporting policy detection as a template" on page 350.

# Password Files policy template

The Password Files policy detects password file formats, such as SAM, password, and shadow.

DCM Rule	Password Filenames
	This rule looks for the file names "passwd" or "shadow."
DCM Rule	/etc/passwd Format
	This rule looks for a regular expression pattern with the /etc/passwd format.
DCM Rule	/etc/shadow Format
	This rule looks for a regular expression pattern with the /etc/shadow format.
DCM Rule	SAM Passwords
	This rule looks for a regular expression pattern with the SAM format.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# Payment Card Industry (PCI) Data Security Standard policy template

The Payment Card Industry (PCI) data security standards are jointly determined by Visa and MasterCard to protect cardholders by safeguarding personally identifiable information. Visa's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection (SDP) program both work toward enforcing these standards. The Payment Card Industry (PCI) Data Security Standards policy detects Visa and MasterCard credit card number data.

The Card Numbers, Exact detection rule detects exact credit card numbers profiled from a database or other data source.

**Table 35-55** Credit Card Numbers, Exact detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	This rule detects credit card numbers.  See "Choosing an Exact Data Profile" on page 322.

The Credit Card Numbers, All detection rule detects credit card numbers using the Credit Card Number system Data Identifier.

Credit Card Numbers. All detection rule Table 35-56

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	Credit Card Numbers, All (Data Identifiers):  Data Identifier: Credit Card Number (narrow) See "Credit Card Number data identifier" on page 715.  Severity: High. Count all matches. Look in envelope, subject, body, attachments.

The Magnetic Stripe Data for Credit Cards detection rule detects raw data from the credit card magnetic stripe using the Credit Card Magnetic Stripe system Data Identifier.

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul> <li>Magnetic Stripe Data for Credit Cards (Data Identifiers):</li> <li>Data Identifier: Credit Card Magnetic Stripe (medium) See "Credit Card Number data identifier" on page 715.</li> <li>Data Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>

Table 35-57 Magnetic Stripe Data for Credit Cards detection rule

See "Exporting policy detection as a template" on page 350.

### PIPEDA policy template

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) protects personal information in the hands of private sector organizations. This act provides guidelines for the collection, use, and disclosure of personal information.

The PIPEDA policy detects customer data that PIPEDA regulations protect.

The PIPEDA detection rule looks for a match of two data items, with certain data combinations excluded from matching.

**Table 35-58** PIPEDA detection rule

Detection method	Description	Excluded combinations
EDM Rule	The PIPEDA detection rule matches any two of the following data items:  Last name Bank card Medical account number Medical record Agency number Account number PIN	However, the following combinations do not create a match:  Last name, email Last name, phone Last name, account number Last name, user name
	<ul> <li>User name</li> <li>Password</li> <li>SIN</li> <li>ABA routing number</li> <li>Email</li> <li>Phone</li> <li>Mother's maiden name</li> </ul> See "Choosing an Exact Data Profile" on page 322.	

The PIPEDA Contact Info detection rule looks for a match of two data items, with certain data combinations excepted from matching.

PIPEDA Contact Info detection rule **Table 35-59** 

Detection method	Description
EDM Rule	This rule looks for any two of the following data columns:  Last name Phone Account number User name Email See "Choosing an Exact Data Profile" on page 322.

Table 35-60	Canadian Social	Incurance Nu	mbers detection rule
Table 35-60	Canadian Social	insurance nui	mbers detection rule

Detection method	Description	
DCM Rule	This rule implements the narrow breadth edition of the Canadian Social Insurance Number data identifier.	
	See "Canadian Social Insurance Number narrow breadth" on page 711.	
	Table 35-61 ABA Routing Numbers detection rule	
Detection method	Description	
DCM Rule	This rule implements the narrow breadth edition of the ABA Routing Number data identifier.	
	See "ABA Routing Number narrow breadth" on page 705.	
	Table 35-62 Credit Card Numbers, All detection rule	
Detection method	Description	
DCM Rule	This rule implements the narrow breadth edition of the Credit Card Number data identifier.	
	See "Credit Card Number narrow breadth" on page 723.	

See "Exporting policy detection as a template" on page 350.

### Price Information policy template

The Price Information policy detects specific SKU and pricing information at risk of exposure.

EDM Rule **Price Information** This rule looks for the combination of user-specified Stock Keeping Unit (SKU) numbers and the price for that SKU number.

Note: This template contains one EDM detection rule. If you do not have an EDM profile configured, or you are using Symantec Data Loss Prevention Standard, this policy template is empty and contains no rule to configure.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

See "About the Exact Data Profile and index" on page 371.

### **Project Data policy template**

The Project Data policy detects discussions of sensitive projects.

**IDM Rule Project Documents, Indexed** 

> This rule looks for content from specific project data files registered as proprietary. It returns a match if the engine detects 80% or more of the

source document.

DCM Rule **Project Activity** 

This rule looks for any keywords in the "Sensitive Project Code Names"

dictionary, which is user-defined.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Proprietary Media Files policy template**

The Proprietary Media Files policy detects various types of video and audio files that can be proprietary intellectual property of your organization at risk for exposure.

IDM Rule Media Files, Indexed

This rule looks for content from specific media files registered as

proprietary.

### DCM Rule **Media Files**

This rule looks for the following media file types:

- qt
- riff
- macromedia dir
- midi
- mp3
- mpeg\_movie
- quickdraw
- realaudio
- wav
- video\_win
- vrml

### DCM Rule **Media Files Extensions**

This rule looks for file name extensions from the "Media Files Extensions" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **Publishing Documents policy template**

The Publishing Documents policy detects various types of publishing documents, such as Adobe FrameMaker files, at risk of exposure.

### IDM Rule **Publishing Documents, Indexed**

This rule looks for content from specific publishing documents registered as proprietary. It returns a match if the engine detects 80% or more of the source document.

DCM Rule

This rule looks for the specified file types:

- qxpress
- frame
- aldus\_pagemaker

**Publishing Documents** 

publ

DCM Rule **Publishing Documents, extensions** 

This rule looks for specified file name extensions found in the "Publishing

Document Extensions" dictionary.

Note: Both file types and file name extensions are required for this policy because the detection engine does not detect the true file type for all the required documents. As such, the file name extension must be used with the file type.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Racist Language policy template

The Racist Language policy detects the use of racist language.

DCM Rule **Racist Language** 

> This rule looks for any single keyword in the "Racist Language" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Restricted Files policy template

The Restricted Files policy detects various file types that are generally inappropriate to send out of the company, such as Microsoft Access and executable files.

DCM Rule **MSAccess Files and Executables** 

This rule looks for files of the specified types: access, exe, and exe\_unix.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Restricted Recipients policy template

The Restricted Recipients policy detects communications with specified recipients, such as former employees.

DCM Rules **Restricted Recipients** 

> This rule looks for messages to recipients with email addresses in the "Restricted Recipients" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Resumes policy template

The Resumes policy detects active job searches.

### EDM Rule Resumes, Employee

This rule is a compound rule with two conditions; both must match to trigger an incident. This rule contains an EDM condition for first and last names of employees provided by the user. This rule also looks for a specific file type attachment (.doc) that is less than 50 KB and contains at least one keyword from each of the following dictionaries:

- Job Search Keywords, Education
- Job Search Keywords, Work
- Job Search Keywords, General

### DCM Rule Resumes, All

This rule looks for files of a specified type (.doc) that are less than 50 KB and match at least one keyword from each of the following dictionaries:

- Job Search Keywords, Education
- Job Search Keywords, Work
- Job Search Keywords, General

### DCM Rule Job Search Websites

This rule looks for URLs of Web sites that are used in job searches.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

See "About the Exact Data Profile and index" on page 371.

### Sarbanes-Oxley policy template

The US Sarbanes-Oxley Act (SOX) imposes requirements on financial accounting, including the preservation of data integrity and the ability to create an audit trail. The Sarbanes-Oxley policy detects sensitive financial data.

The Sarbanes-Oxley Documents, Indexed detection rule looks for content from specific documents registered as being subject to Sarbanes-Oxley Act. This rule returns a match if 80% or more of the source document is found.

Table 35-63 Sarbanes-Oxley Documents, Indexed detection rule

Method	Condition	Configuration
Simple rule	Content Matches Indexed Document Profile	See "Choosing an Indexed Document Profile" on page 323.

The SEC Fair Disclosure Regulation compound detection rule looks for the following conditions; all must be satisfied for the rule to trigger an incident:

- The SEC Fair Disclosure keywords indicate possible disclosure of advance financial information ("SEC Fair Disclosure Keywords" dictionary).
- An attachment or file type that is a commonly used document or spreadsheet format. The detected file types are Microsoft Word, Excel Macro, Excel, Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro, WordPerfect, Lotus 123, Applix Spreadsheets, CSV, Multiplan Spreadsheet, and Adobe PDF.
- The company name keyword list requires editing by the user, which can include any name, alternate name, or abbreviation that might indicate a reference to the company.

Table 35-64 SEC Fair Disclosure Regulation detection rule

Method	Condition	Configuration
	Content Matches Keyword	SEC Fair Disclosure Regulation (Keyword Match):  Match keyword: earnings per share, forward guidance Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only. Match on same component. The keyword must be in the attachment or file type detected by that condition.
	Message Attachment or File Type Match	SEC Fair Disclosure Regulation (Attachment/File Type):  File type detected: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, and pdf.  Severity: High.  Match on: Attachments and same component.
	Content Matches Keyword	SEC Fair Disclosure Regulation (Keyword Match):  Match "[company name]" Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only. Match on same component. The keyword must be in the attachment or file type detected by that condition.

The Financial Information detection rule looks for a specific file type containing a word from the "Financial Keywords" dictionary and a word from the "Confidential/Proprietary Words" dictionary. The spreadsheet file types detected are Microsoft Excel Macro, Microsoft Excel, Microsoft Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro, and more.

Method	Condition	Configuration		
Compound rule	Content Matches Indexed Document Profile	Financial Information (Attachment/File Type):  Match file type: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, Lotus 1-2-3  Severity: High.  Match on attachments, same component.		
	Content Matches Keyword	<ul> <li>Financial Information (Keyword Match):</li> <li>Match "accounts receivable turnover", "adjusted gramargin", "adjusted operating expenses", "adjusted operating margin", "administrative expenses",</li> <li>Severity: High.</li> <li>Check for existence.</li> <li>Look in envelope, subject, body, attachments.</li> <li>Case insensitive.</li> <li>Match on whole words only.</li> <li>Keyword must be detected in the attachment (san component).</li> </ul>		
	Content Matches Keyword	Financial Information (Keyword Match):  Match "confidential", "internal use only", "proprietary".  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments.  Case insensitive.  Match on whole words only.  Keyword must be detected in the attachment (same component).		

**Table 35-65** Financial Information detection rule

See "Exporting policy detection as a template" on page 350.

# **SEC Fair Disclosure Regulation policy template**

The US SEC Selective Disclosure and Insider Trading Rules prohibit public companies from selectively divulging material information to analysts and institutional investors before its general release to the public.

The SEC Fair Disclosure Regulation template detects data indicating disclosure of material financial information.

The SEC Fair Disclosure Regulation Documents, Indexed (IDM) detection rule looks for content from specific documents subject to SEC Fair Disclosure regulation. This rule returns a match if 80% or more of the source document content is found.

Table 35-66 SEC Fair Disclosure Regulation Documents, Indexed (IDM) detection rule

Method	Condition	Configuration
Simple rule	Content Matches Document Signature (IDM)	SEC Fair Disclosure Regulation Documents, Indexed (IDM):  Detect documents from the selected Indexed Document Profile. See "Choosing an Indexed Document Profile" on page 323.  Match documents with at least 80% content match. Severity: High. Check for existence. Look in body, attachments.

The SEC Fair Disclosure Regulation detection rule looks for the a keyword match from the "SEC Fair Disclosure Keywords" dictionary, an attachment or file type that is a commonly used document or spreadsheet, and a keyword match from the "Company Name Keywords" dictionary.

All three conditions must be satisfied for the rule to trigger an incident:

- The SEC Fair Disclosure keywords indicate possible disclosure of advance financial information.
- The file types detected are Microsoft Word, Excel Macro, Excel, Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro, WordPerfect, Lotus 123, Applix Spreadsheets, CSV, Multiplan Spreadsheet, and Adobe PDF.
- The company name keyword list requires editing by the user, which can include any name, alternate name, or abbreviation that might indicate a reference to the company.

Method	Condition	Configuration
Compound rule	Content Matches Keyword (DCM)	SEC Fair Disclosure Regulation (Keyword Match):  Match "earnings per share", "forward guidance".  Severity: High. Check for existence. Look in envelope, subject, body, attachments.  Case insensitive. Match on whole words only.
	Message Attachment or File Type Match (DCM)	SEC Fair Disclosure Regulation (Attachment/File Type):  Match file type: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, pdf Severity: High. Match on attachments. Require content match to be in the same component (attachment).
	Content Matches Keyword (DCM)	SEC Fair Disclosure Regulation (Keyword Match):  Match "[company name]" (user defined)  Severity: High.  Check for existence.  Look in envelope, subject, body, attachments, same component.  Case insensitive.  Match on whole words only.

**Table 35-67** SEC Fair Disclosure Regulation detection rule

See "Exporting policy detection as a template" on page 350.

# **Sexually Explicit Language policy template**

The Sexually Explicit Language policy detects vulgar, sexually explicit, and pornographic language content.

DCM Rule Sexually Explicit Keywords, Confirmed

> This rule looks for any single keyword in the "Sex. Explicit Keywords, Confirmed" dictionary.

DCM Rule Sexually Explicit Keywords, Suspected

This rule looks for any three instances of keywords in the "Sex. Explicit

Words, Suspect" dictionary.

DCM Rule Sexually Explicit Keywords, Possible

This rule looks for any three instances of keywords in the "Sex. Explicit

Words, Possible" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

# Source Code policy template

The Source Code policy template provides match conditions for detecting various types of source code at risk of exposure, including C, Java, Perl, and Visual Basic (VB).

Source code policy template match conditions **Table 35-68** 

Name	Туре	Description
Source Code Documents	IDM	This rule looks for specific user-provided source code from a <b>Document Profile</b> .
		This rule returns a match if it detects 80% or more of the source document.
		This rule is not available if you do not select a profile when creating the policy.
Source Code Extensions	File Name Match	This rule looks for a match among file name extensions from the "Source Code Extensions" dictionary.
Java Source Code	Regular Expressions	This compound rule looks for matches on two different regular expression patterns: Java Import Statements and Java Class Files.
C Source Code	Regular Expression	This rule looks for matches on the C Source Code regular expression pattern.
VB Source Code	Regular Expression	This rule looks for matches on the VB Source Code regular expression pattern.
Perl Source Code	Regular Expressions	This compound rule looks for matches on three different Perl-related regular expressions patterns.

See "Exporting policy detection as a template" on page 350.

### State Data Privacy policy template

Many states in the US have adopted statutes mandating data protection and public disclosure of information security breaches in which confidential data of individuals is compromised. The State Data Privacy policy template is designed to address these types of confidential data breaches.

The State Data Privacy policy template provides several individual detection rules and produces an incident if any of these rules are violated. This policy template also provides a configurable exception condition that allows one or more authoriezed email recipients to receive otherwise confidential data.

Table 35-69 describes the acceptable use condition implemented by the State Data Privacy policy. You must configure the exception for it to apply.

Name Type Description **Configuration details** Fmail to Described Email to Affiliates is a policy exception that allows Simple exception (single Affiliates identity (DCM) email messages to be sent to affiliates who are condition) (Recipient) legitimately allowed to receive information Match email recipient: Recipient covered under the State Data Privacy regulations. [affiliate1], [affiliate2]. Matches Pattern Edit the "Affiliate Domains" Policy exceptions are evaluated before detection list and enter the email match conditions. If there is an exception, in this address for each recipient case an affiliate email address that you have who may make acceptable entered, the entire message is discarded and not use of the confidential data. available for evaluation by detection. At least 1 recipient(s) must match for the exception to trigger. Matches on the entire message.

Email to Affiliates policy exception **Table 35-69** 

The State Data Privacy policy templated implements Exact Data Matching (Table 35-70). If you do not select an **Exact Data** profile when you first create a policy based on this template, the EDM condition is not available for use.

See "Choosing an Exact Data Profile" on page 322.

Table 35-70	State Data Privacy EDM rule
-------------	-----------------------------

Rule name	Condition type	Description	Configuration details
State Data Privacy, Consumer Data	Content matches Exact Data (EDM)	This rule looks for an exact data match on three of the following:  ABA Routing Number  Account Number  Bank Card Number (credit card number)  Birth Date  Driver License Number  First Name  Last Name  Password  PIN Number  Social Security Number  State ID Card Number  Exception conditions: the following combinations do not match:  First Name, Last Name, PlN  First Name, Last Name, Password	When you are creating the EDM profile, you should validate it against the State Data Privacy template to ensure that the resulting index includes expected fields.  Simple rule (single match condition) Severity: High Report incident if 1 match Look in envelope, body, attachments

Table 35-71 lists and describes the DCM detection rules implemented by the State Data Privacy policy. If any one of these rules is violated the policy produces an incident, unless you have configured the exception condition and the message recipient is an acceptable use affiliate.

State Data Privacy detection rules Table 35-71

Rule name	Condition type	Description	Configuration details
US Social Security Number Patterns	Content Matches Data Identifier (DCM)	The US Social Security Number Patterns rule is designed to detect US social security numbers (SSNs). The Randomized US SSN data identifier detects SSN patterns, both traditional and those issued under the new randomization scheme.  See "Randomized US Social Security Number (SSN) data identifier" on page 759.	<ul> <li>Simple rule (single match condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>

State Data Privacy detection rules (continued) Table 35-71

Rule name	Condition type	Description	Configuration details
ABA Routing Numbers	Content Matches Data Identifier (DCM)	The ABA Routing Numbers rule is designed to detect ABA Routing Numbers.  The ABA Routing Numbers data identifier detects ABA routing numbers.  See "ABA Routing Number narrow breadth" on page 705.	<ul> <li>Simple rule (single match condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments.</li> </ul>
Credit Card Numbers, All	Content Matches Data Identifier (DCM)	The Credit Card Numbers rule is designed to match on credit card numbers.  To detect credit card numbers, this rule implements the Credit Card Number narrow breadth system data identifier.  See "Credit Card Number narrow breadth" on page 723.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>
CA Drivers License Numbers	Content Matches Data Identifier (DCM)	The CA Drivers License Numbers rule looks for a match for the CA drivers license number pattern, a match for a data identifier for terms relating to "drivers license," and a keyword from the "California Keywords" dictionary.  See "Drivers License Number – CA State data identifier" on page 730.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>
NY Drivers License Numbers	Content Matches Data Identifier (DCM)	The NY Drivers License Numbers rule looks for a match for the NY drivers license number pattern, a match for a regular expression for terms relating to "drivers license," and a keyword from the "New York Keywords" dictionary.  See "Drivers License Number - NY State data identifier" on page 740.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>
FL, MI, and MN Drivers License Numbers	Content Matches Data Identifier (DCM)	The FL, MI, and MN Drivers License Numbers rule looks for a match for the stated drivers license number pattern, a match for a regular expression for terms relating to "drivers license," and a keyword from the "Letter/12 Num. DLN State Words" dictionary (namely, Florida, Minnesota, and Michigan).  See "Drivers License Number - FL, MI, MN States data identifier" on page 732.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>

Rule name	Condition type	Description	Configuration details
IL Drivers License Numbers	Content Matches Data Identifier (DCM)	The IL Drivers License Numbers detection rule looks for a match for the IL drivers license number pattern, a match for a regular expression for terms relating to "drivers license," and a keyword from the "Illinois Keywords" dictionary.  See "Drivers License Number - IL State data identifier" on page 735.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>
NJ Drivers License Numbers	Content Matches Data Identifier (DCM)	The NJ Drivers License Numbers detection rule looks for a match for the NJ drivers license number pattern, a match for a regular expression for terms relating to "drivers license," and a keyword from the "New Jersey Keywords" dictionary.  This condition implements the Driver's License Number- NJ State medium breadth system Data Identifier.  See "Drivers License Number- NJ State medium breadth" on page 739.	<ul> <li>Simple rule (single condition)</li> <li>Severity: High.</li> <li>Count all matches.</li> <li>Look in envelope, subject, body, attachments</li> </ul>

Table 35-71 State Data Privacy detection rules (continued)

See "Exporting policy detection as a template" on page 350.

### **SWIFT Codes policy template**

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a cooperative organization under Belgian law and is owned by its member financial institutions. The SWIFT code (also known as a Bank Identifier Code, BIC, or ISO 9362) has a standard format to identify a bank, location, and the branch involved. These codes are used when transferring money between banks, particularly across international borders.

DCM Rule **SWIFT Code Regular Expression** 

> This rule looks for a match to the SWIFT code regular expression and a keyword from the "SWIFT Code Keywords" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Symantec DLP Awareness and Avoidance policy template

The Symantec DLP Awareness & Avoidance policy detects any communications that refer to Symantec Data Loss Prevention or data loss prevention systems and possible avoidance of detection. The Symantec DLP Awareness & Avoidance policy is most useful for the deployments that are not widely known among monitored users.

DCM Rule **Symantec DLP Awareness** 

Checks for a keyword match from the "Symantec DLP Awareness"

dictionary.

DCM Rule **Symantec DLP Avoidance** 

> This rule is a compound rule with two conditions: both must be matched to trigger an incident. This rule looks for a keyword match from the "Symantec DLP Awareness" dictionary and a keyword from the

"Symantec DLP Avoidance" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **UK Drivers License Numbers policy template**

The UK Drivers License Numbers policy detects UK Drivers License Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.

### DCM Rule **UK Drivers License Numbers**

This rule is a compound rule with the following conditions:

- A single keyword from the "UK Keywords" dictionary
- The pattern matching that of the UK drivers license data identifier
- Different combinations of the phrase "drivers license" using a data identifier

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### UK Electoral Roll Numbers policy template

The UK Electoral Roll Numbers policy detects UK Electoral Roll Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.

DCM Rule

**UK Electoral Roll Numbers** 

This rule is a compound rule with the following conditions:

- A single keyword from the "UK Keywords" dictionary
- A pattern matching the UK Electoral Roll Number data identifier
- A single keyword from the "UK Electoral Roll Number Words" dictionary

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### UK National Health Service (NHS) Number policy template

The UK National Health Service (NHS) Number policy detects the personal identification number issued by the U.K. National Health Service (NHS) for administration of medical care.

DCM Rule

**UK NHS Numbers** 

This rule looks for a single compound condition with two parts: either new or old style National Health Service numbers and a single keyword from the "UK NHS Keywords" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **UK National Insurance Numbers policy template**

The National Insurance Number is issued to individuals by the UK Department for Work and Pensions and Inland Revenue (DWP/IR) for administering the national insurance system. The UK National Insurance Numbers policy detects these insurance policy numbers.

DCM Rule **UK National Insurance Numbers** 

> This rule looks for a match to the UK National Insurance number data identifier and a keyword from the dictionary "UK NIN Keywords."

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

#### **UK Passport Numbers policy template**

The UK Passport Numbers policy detects valid UK passports using the official specification of the UK Government Standards of the UK Cabinet Office.

DCM Rule **UK Passport Numbers (Old Type)** 

> This rule looks for a keyword from the "UK Passport Keywords" dictionary and a pattern matching the regular expression for UK Passport

Numbers (Old Type).

DCM Rule **UK Passport Numbers (New Type)** 

> This rule looks for a keyword from the "UK Passport Keywords" dictionary and a pattern matching the regular expression for UK Passport

Numbers (New Type).

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **UK Tax ID Numbers policy template**

The UK Tax ID Numbers policy detects UK Tax ID Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.

DCM Rule **UK Tax ID Numbers** 

This rule looks for a match to the UK Tax ID number data identifier and

a keyword from the dictionary "UK Tax ID Number Keywords."

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## **US Intelligence Control Markings (CAPCO) and DCID** 1/7 policy template

The US Intelligence Control Markings (CAPCO) & DCID 1/7 policy detects authorized terms to identify classified information in the US Federal Intelligence community as defined in the Control Markings Register, which is maintained by the Controlled Access Program Coordination Office (CAPCO) of the Community Management Staff (CMS). The register was created in response to the Director of Central Intelligence Directive (DCID) 1/7.

This rule looks for a keyword match on the phrase "TOP SECRET."

Table 35-72 Top Secret Information detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "TOP SECRET//"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case sensitive. Match on whole or partial words.

This rule looks for a keyword match on the phrase "SECRET."

Secret Information detection rule **Table 35-73** 

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "SECRET//"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case sensitive. Match on whole or partial words.

This rule looks for a keyword match on the phrases "CLASSIFIED" or "RESTRICTED."

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "CLASSIFIED//,//RESTRICTED//"  Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case sensitive. Match on whole or partial words.

Table 35-74 Classified or Restricted Information (Keyword Match) detection rule

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### **US Social Security Numbers policy template**

The US Social Security Numbers policy detects patterns indicating social security numbers at risk of exposure.

Table 35-75 US Social Security Numbers policy template

Rule name	Rule type	Description	Details
US Social Security Number Patterns	DCM Rule	This rule looks for a match to the social security number regular expression and a keyword from the dictionary "US SSN Keywords."	See "Randomized US Social Security Number (SSN) data identifier" on page 759.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

#### Violence and Weapons policy template

The Violence and Weapons policy detects violent language and discussions about weapons.

**Table 35-76** Violence and Weapons policy template

Name	Туре	Description
Violence and Weapons	DCM Rule	This rule is a compound rule with two conditions; both must match to trigger an incident. This rule looks for a keyword from the "Violence Keywords" dictionary and a keyword from the "Weapons Keywords" dictionary.

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

## Webmail policy template

The Webmail policy detects the use of a variety of Webmail services, including Yahoo, Google, and Hotmail.

Table 35-77 Webmail policy template rules

Name	Туре	Condition(s)	Description
Yahoo	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL domain mail.yahoo.com.
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>ym/compose</b> .
Hotmail	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL domain hotmail.msn.com.
		Content Matches Keyword (DCM)	This condition checks for the keyword compose?&curmbox.
	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL <b>gomailus.go.com</b> .
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>compose</b> .
AOL Compound detection rule		Recipient Matches Pattern (DCM)	This condition checks for the URL domain aol.com.
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>compose</b> .
Gmail	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL domain gmail.google.com.
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>gmail</b> .

See "Configuring policies" on page 326.

See "Exporting policy detection as a template" on page 350.

### Yahoo Message Board Activity policy template

The Yahoo Message Board policy template detects Yahoo message board activity.

The Yahoo Message Board detection rule is a compound method that looks for messages posted to the Yahoo message board you specify.

Table 35-78 describes its configuration details.

Table 35-78 Yahoo Message Board detection rule

Method	Condition	Configuration			
Compound rule	Content Matches Keyword (DCM)	Yahoo Message Board (Keyword Match):  Case insensitive.  Match Keyword: post.messages.yahoo.com/bbs.  Match on whole words only.  Check for existence (do not count multiple matches).  Look in envelope, subject, body, attachments.  Match must occur in the same component for both conditions.			
	AND				
	Content Matches Keyword (DCM)	Yahoo Message Board (Keyword Match):  Case insensitive.  Match Keyword: board= <enter board="" number="">.  Match on whole words only.  Check for existence (do not count multiple matches).  Look in envelope, subject, body, attachments.  Match must occur in the same component for both conditions.</enter>			

The Finance Message Board URL detection rule detects messages posted to the Yahoo Finance message board.

Table 35-79 describes its configuration.

Table 35-79	Finance	Message	Roard	HRI	detection	rule
1 able 33-73	Illiance	Message	Duaru	OIL	detection	luic

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Finance Message Board URL (Keyword Match):  Case insensitive.  Match Keyword: messages.finance.yahoo.com.  Match on whole words only.  Check for existence (do not count multiple matches).  Look in envelope, subject, body, attachments.

The Board URLs detection rule detects messages posted to the Yahoo or Yahoo Finance message boards by the URL of either.

Table 35-80 describes its configuration details.

Board URLs detection rule Table 35-80

Method	Condition	Configuration
Simple rule	Recipient Matches Pattern (DCM)	Board URLs (Recipient):  Recipient URL: messages.yahoo.com,messages.finance.yahoo.com.  At least 1 recipient(s) must match.  Matches on the entire message (not configurable).

See "Creating a policy from a template" on page 312.

See "Exporting policy detection as a template" on page 350.

## Yahoo and MSN Messengers on Port 80 policy template

The Yahoo and MSN Messengers on Port 80 policy detects Yahoo and MSN Messenger activity over port 80.

The Yahoo IM detection rule looks for keyword matches on both ymsg and shttp.msg.yahoo.com.

Table 35-81 Yahoo IM detection rule

Method	Condition	Configuration		
	Content Matches Keyword (DCM)	Yahoo IM (Keyword Match):  Case insensitive.  Match keyword: ymsg.  Match on whole words only.  Count all matches and report an incident for each match.  Look for matches in the envelope, subject, body, and attachments.  Match must occur in the same component for both conditions in the rule.		
Compound rule	AND			
	Content Matches Keyword (DCM)	Yahoo IM (Keyword Match):  Case insensitive.  Match keyword: shttp.msg.yahoo.com.  Match on whole words only.  Count all matches and report an incident for each match.  Look for matches in the envelope, subject, body, and attachments.  Match must occur in the same component for both conditions in the rule.		

The MSN IM detection rule looks for matches on three keywords in the same message component.

Table 35-82	MSN IM detection rule
Table 33"oz	MON IN REFERENCE IN THE

Method	Condition	Configuration
	Content Matches Keyword (DCM)	MSN IM (Keyword Match):  Case insensitive.  Match keyword: msg.  Match on whole words only.  Count all matches and report an incident for each match.  Look for matches in the envelope, subject, body, and attachments.  Match must occur in the same component for all conditions in the rule.
	AND	
Compound rule	Content Matches Keyword (DCM)	MSN IM (Keyword Match):  Case insensitive.  Match keyword: x-msn.  Match on whole words only.  Count all matches and report an incident for each match.  Look for matches in the envelope, subject, body, and attachments.  Match must occur in the same component for all conditions in the rule.
	AND	
	Content Matches Keyword (DCM)	MSN IM (Keyword Match):  Case insensitive.  Match keyword: charset=utf-8.  Match on whole words only.  Count all matches and report an incident for each match.  Look for matches in the envelope, subject, body, and attachments.  Match must occur in the same component for all conditions in the rule.

See "Creating a policy from a template" on page 312.

See "Exporting policy detection as a template" on page 350.

Section

# Configuring policy response rules

- Chapter 36. Responding to policy violations
- Chapter 37. Configuring and managing response rules
- Chapter 38. Response rule conditions
- Chapter 39. Response rule actions

## Responding to policy violations

This chapter includes the following topics:

- About response rules
- About response rule actions
- Response rules for all detection servers
- Response rules for endpoint detection
- Response rules for Network and Mobile Prevent for Web detection
- Response rules for Network Protect detection
- Response rule for the Classification Server
- About response rule execution types
- About Automated Response rules
- About Smart Response rules
- About response rule conditions
- About response rule action execution priority
- About response rule authoring privileges
- Implementing response rules
- Response rule best practices

#### About response rules

You can implement one or more response rules in a policy to escalate, resolve, and dismiss incidents when a violation occurs. For example, if a policy is violated, a response rule blocks the transmission of a file containing sensitive content.

See "About response rule actions" on page 875.

You create, modify, and manage response rules separate from the policies that declare them. This decoupling allows response rules to be updated and reused across policies.

See "Implementing response rules" on page 886.

The detection server automatically executes response rules. Or, you can configure Smart Response rules for manual execution by an incident remediator.

See "About response rule execution types" on page 880.

You can implement conditions to control how and when response rules execute.

See "About response rule conditions" on page 882.

You can sequence the order of execution for response rules of the same type.

See "About response rule action execution priority" on page 883.

You must have response rule authoring privileges to create and manage response rules.

See "About response rule authoring privileges" on page 885.

### About response rule actions

Response rule actions are the components that take action when a policy violation occurs. Response rule actions are mandatory components of response rules. If you create a response rule, you must define at least one action for the response rule to be valid.

Symantec Data Loss Prevention provides several response rule actions. Many are available for all types of detection servers. Others are available for specific detection servers.

See "Implementing response rules" on page 886.

The detection server where a policy is deployed executes a response rule action any time a policy violation occurs. Or, you can configure a response rule condition to dictate when the response rule action executes.

See "About response rule conditions" on page 882.

For example, anytime a policy is violated, send an email to the user who violated the policy and the manager. Or, if a policy violation severity level is medium, present the user with an on-screen warning. Or, if the severity is high, block a file from being copied to an external device.

**Table 36-1** Response rules by server type

Server type	Description
All detection servers	See "Response rules for all detection servers" on page 876.
Endpoint detection servers	See "Response rules for endpoint detection" on page 877.
Network and Mobile Prevent for Web detection servers	See "Response rules for Network and Mobile Prevent for Web detection" on page 878.
Network Protect detection servers	See "Response rules for Network Protect detection" on page 879.
Classification detection server	See "Response rule for the Classification Server" on page 880.

### Response rules for all detection servers

Symantec Data Loss Prevention provides several response rule actions for Endpoint Prevent, Endpoint Discover, Network Prevent for Web, Network Prevent for Email, Mobile Prevent for Web, and Network Protect.

Available response rules for all detection servers **Table 36-2** 

Response rule	Description
Add Note	Add a field to the incident record that the remediator can annotate at the <b>Incident Snapshot</b> screen.
	See "Configuring the Add Note action" on page 906.
Limit Incident Data Retention	Discard or retain matched data with the incident record.
	See "Configuring the Limit Incident Data Retention action" on page 906.
Log to a Syslog Server	Log the incident to a syslog server.
	See "Configuring the Log to a Syslog Server action" on page 909.
Send Email Notification	Send an email you compose to recipients you specify.
	See "Configuring the Send Email Notification action" on page 910.

Response rule	Description
Server FlexResponse	Execute a custom Server FlexResponse action.
	See "Configuring the Server FlexResponse action" on page 912.
	<b>Note:</b> This response rule action is available only if you deploy one or more custom Server FlexResponse plug-ins to Symantec Data Loss Prevention.
	See "Deploying a Server FlexResponse plug-in" on page 1231.
Set Attribute	Add a custom value to the incident record.
	See "Configuring the Set Attribute action" on page 913.
Set Status	Change the incident status to the specified value.
	See "Configuring the Set Status action" on page 914.

**Table 36-2** Available response rules for all detection servers (continued)

See "About response rules" on page 875.

See "Implementing response rules" on page 886.

## Response rules for endpoint detection

Symantec Data Loss Prevention provides several response rule actions for Endpoint Prevent and Endpoint Discover.

**Table 36-3** Available Endpoint response rules

Response rule	Description
Endpoint: FlexResponse	Take custom action using the FlexResponse API.
	See "Configuring the Endpoint: FlexResponse action" on page 919.
Endpoint Discover: Quarantine File	Quarantine a discovered sensitive file.
	See "Configuring the Endpoint Discover: Quarantine File action" on page 920.
Endpoint Prevent: Block	Block the transfer of data that violates the policy.
	For example, block the copy of confidential data from an endpoint to a USB flash drive.
	See "Configuring the Endpoint Prevent: Block action" on page 922.
Endpoint Prevent: Notify	Display an on-screen notification to the endpoint user when confidential data is transferred.
	See "Configuring the Endpoint Prevent: Notify action" on page 924.

Response rule	Description
Endpoint Prevent: User Cancel	Allow the user to cancel the transfer of a confidential file. The override is time sensitive.
	See "Configuring the Endpoint Prevent: User Cancel action" on page 928.

**Table 36-3** Available Endpoint response rules (continued)

See "About response rules" on page 875.

See "Implementing response rules" on page 886.

#### Response rules for Network and Mobile Prevent for Web detection

Symantec Data Loss Prevention provides several response rule actions for Network Prevent for Web, Network Prevent for Email, and Mobile Prevent for Web.

**Table 36-4** Available Network response rules

Response rule	Description	
Network Prevent: Block FTP Request	Block FTP transmissions.	
	See "Configuring the Network and Mobile Prevent for Web: Block FTP Request action" on page 931.	
	Note: Only available with Network Prevent for Web.	
Network Prevent: Block HTTP/S	Block Web postings.	
	See "Configuring the Network and Mobile Prevent for Web: Block HTTP/S action" on page 931.	
	<b>Note:</b> Only available with Network Prevent for Web.	
Network Prevent: Block SMTP Message	Block email that causes an incident.	
(Network Prevent only)	See "Configuring the Network Prevent: Block SMTP Message action" on page 933.	
	Note: Only available with Network Prevent for Email.	

Response rule	Description
Network Prevent: Modify SMTP Message (Network Prevent only)	Modify sensitive email messages.
	For example, change the email subject to include information about the violation.
	See "Configuring the Network Prevent: Modify SMTP Message action" on page 934.
	Note: Only available with Network Prevent for Email.
Network Prevent: Remove HTTP/S	Remove confidential content from Web posts.
Content	See "Configuring the Network and Mobile Prevent for Web: Remove HTTP/S Content action" on page 935.
	Note: Only available with Network Prevent for Web.

**Table 36-4** Available Network response rules (continued)

See "About response rules" on page 875.

See "Implementing response rules" on page 886.

### Response rules for Network Protect detection

Symantec Data Loss Prevention provides several response rule actions for Network Protect (Discover).

**Table 36-5** Available Network Protect response rules

Response rule	Description
Network Protect: Copy File	Copy sensitive files to a location you specify.  See "Configuring the Network Protect: Copy File action" on page 937.  Note: Only available with Network Protect.
Network Protect: Quarantine File	Quarantine sensitive files.  See "Configuring the Network Protect: Quarantine File action" on page 937.  Note: Only available with Network Protect.

See "About response rules" on page 875.

See "Implementing response rules" on page 886.

#### Response rule for the Classification Server

The Classify Enterprise Vault Content response rule uses a Classification Server to automatically classify, archive, or delete Exchange messages with Enterprise Vault for Microsoft Exchange.

Note: This response rule is used only with the Symantec Data Classification for Enterprise Vault solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Enterprise Vault Data Classification Services filter and Classification Server to communicate with one another. See the Enterprise Vault Data Classification Services Implementation Guide for more information.

Table 36-6	Available Classification response rule
Response rule	Description
Classification: Classify Enterprise Vault Content	Defines the classification result tags and retention categories that Symantec Enterprise Vault for Microsoft Exchange uses to archive, delete, or flag Exchange messages for compliance reviews and E-Discovery searches.
	See "Configuring the Classify Enterprise Vault Content response action" on page 915.
	The Classification Server delivers the retention category and classification tag to the Data Classification for Enterprise Vault filter that delivered the message for detection. The classification tag corresponds to the name of the policy that executed the response rule.

See "About response rules" on page 875.

See "Implementing response rules" on page 886.

#### About response rule execution types

Symantec Data Loss Prevention provides two types of policy response rules: Automated and Smart.

The detection server that reports a policy violation executes Automated Response rules. Users such as incident remediators execute Smart Response rules on demand from the Enforce Server administration console.

See "About recommended roles for your organization" on page 88.

Response rule execution type	Description
Automated Response rules	When a policy violation occurs, the detection server automatically executes response rule actions.  See "About Automated Response rules" on page 881.
Smart Response rules	When a policy violation occurs, an authorized user manually triggers the response rule.  See "About Smart Response rules" on page 881.

**Table 36-7** Response rule types

See "About response rule actions" on page 875.

See "Implementing response rules" on page 886.

#### About Automated Response rules

The system executes Automated Response rules when the detection engine reports a policy violation. However, if you implement a response rule condition, the condition must be met for the system to execute the response rule. Conditions let you control the automated execution of response rule actions.

See "About response rule conditions" on page 882.

For example, the system can automatically block certain policy violating actions, such as the attempted transfer of high value customer data or sensitive design documents. Or, the system can escalate an incident to a workflow management system for immediate attention. Or, you can set a different severity level for an incident involving 1000 customer records than for one involving only 10 records.

See "Implementing response rules" on page 886.

#### **About Smart Response rules**

Users execute Smart Response rules on demand in response to policy violations from the Enforce Server administration console Incident Snapshot screen.

See "About response rule actions" on page 875.

You create Smart Response rules for the situations that require human remediation. For example, you might create a Smart response rule to dismiss false positive incidents. An incident remediator can review the incident, identify the match as a false positive, and dismiss it.

See "About configuring Smart Response rules" on page 892.

Only some response rules are available for manual execution.

**Table 36-8** Available Smart Response rules for manual execution

Smart response rule	Description
Add Note	Add a field to the incident record that the remediator can annotate at the <b>Incident Snapshot</b> screen.
	See "Configuring the Add Note action" on page 906.
Log to a Syslog Server	Log the incident to a syslog server for workflow remediation.
	See "Configuring the Log to a Syslog Server action" on page 909.
Send Email Notification	Send an email you compose to recipients you specify.
	See "Configuring the Send Email Notification action" on page 910.
Server FlexResponse	Execute a custom Server FlexResponse action.
	See "Configuring the Server FlexResponse action" on page 912.
	<b>Note:</b> This response rule action is available only if you deploy one or more custom Server FlexResponse plug-ins to Symantec Data Loss Prevention.
	See "Deploying a Server FlexResponse plug-in" on page 1231.
Set Status	Set the incident status to the specified value.
	See "Configuring the Set Status action" on page 914.

See "Implementing response rules" on page 886.

#### About response rule conditions

Response rule conditions are optional response rule components. Conditions define how and when the system triggers response rule actions. Conditions give you multiple ways to prioritize incoming incidents to focus remediation efforts and take appropriate response.

See "Implementing response rules" on page 886.

Response rule conditions trigger action based on detection match criteria. For example, you can configure a condition to trigger action for high severity incidents, certain types of incidents, or after a specified number of incidents.

See "Configuring response rule conditions" on page 892.

Conditions are not required. If a response rule does not declare a condition, the response rule action always executes each time an incident occurs. If a condition is declared, it must be met for the action to trigger. If more than one condition is declared, all must be met for the system to take action.

See "Configuring response rules" on page 891.

**Table 36-9** Available response rule conditions

Condition type	Description
Endpoint Location	Triggers a response action when the endpoint is on or off the corporate network.  See "Configuring the Endpoint Location response condition" on page 897.
Endpoint Device	Triggers a response action when an event occurs on a configured endpoint device.  See "Configuring the Endpoint Device response condition" on page 898.
Incident Type	Triggers a response action when the specified type of detection server reports a match.  See "Configuring the Incident Type response condition" on page 899.
Incident Match Count	Triggers a response action when the volume of policy violations exceeds a threshold or range.  See "Configuring the Incident Match Count response condition" on page 900.
Protocol or Endpoint Monitoring	Triggers a response action when an incident is detected on a specified network communications protocol (such as HTTP) or endpoint destination (such as CD/DVD).  See "Configuring the Protocol or Endpoint Monitoring response condition" on page 901.
Severity	Triggers a response action when the policy violation is a certain severity level.  See "Configuring the Severity response condition" on page 903.

#### About response rule action execution priority

A Symantec Data Loss Prevention server executes response rule actions according to a system-defined prioritized order. You cannot modify the order of execution among response rules of different types.

In all cases, when a server executes two or more different response rules for the same policy, the higher priority response action takes precedence.

Consider the following example(s):

 One endpoint response rule lets a user cancel an attempted file copy and another rule blocks the attempt.

The detection server blocks the file copy.

One network response rule action copies a file and another action quarantines

The detection server quarantines the file.

 One network response rule action modifies the content of an email message and another action blocks the transmission.

The detection server blocks the email transmission.

You cannot change the priority execution order for different response rule action types. But, you can modify the order of execution for the same type of response rule action with conflicting instructions.

See "Modifying response rule ordering" on page 895.

Table 36-10 System-defined response rule execution priority

Execution priority	Description
(from highest to lowest)	·
Endpoint Prevent: Block	See "Configuring the Endpoint Prevent: Block action" on page 922.
Endpoint Prevent: User Cancel	See "Configuring the Endpoint Prevent: User Cancel action" on page 928.
Endpoint: FlexResponse	See "Configuring the Endpoint: FlexResponse action" on page 919.
Endpoint Prevent: Notify	See "Configuring the Endpoint Prevent: Notify action" on page 924.
Endpoint Discover: Quarantine File	See "Configuring the Endpoint Discover: Quarantine File action" on page 920.
Limit Incident Data Retention	See "Configuring the Limit Incident Data Retention action" on page 906.
Network Prevent: Block SMTP Message	See "Configuring the Network Prevent: Block SMTP Message action" on page 933.
Network Prevent: Modify SMTP Message	See "Configuring the Network Prevent: Modify SMTP Message action" on page 934.
Network and Mobile Prevent for Web: Remove HTTP/HTTPS Content	See "Configuring the Network and Mobile Prevent for Web: Remove HTTP/S Content action" on page 935.

**Execution priority** Description (from highest to lowest) Network and Mobile Prevent for See "Configuring the Network and Mobile Prevent for Web: Block HTTP/HTTPS Web: Block HTTP/S action" on page 931. Network and Mobile Prevent for See "Configuring the Network and Mobile Prevent for Web: Block FTP Request Web: Block FTP Request action" on page 931. Network Protect: Quarantine File See "Configuring the Network Protect: Quarantine File action" on page 937. Network Protect: Copy File See "Configuring the Network Protect: Copy File action" on page 937. See "Configuring the Classify Enterprise Vault Content Classify Content response action" on page 915. Set Status See "Configuring the Set Status action" on page 914. Set Attribute See "Configuring the Set Attribute action" on page 913. Add Note See "Configuring the Add Note action" on page 906. Log to a Syslog Server See "Configuring the Log to a Syslog Server action" on page 909. Send Email Notification See "Configuring the Send Email Notification action" on page 910. Server FlexResponse See "Configuring the Server FlexResponse action" on page 912. Note: Server FlexResponse actions that are part of Automated Response rules execute on the Enforce Server, rather than the detection server.

Table 36-10 System-defined response rule execution priority (continued)

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

#### About response rule authoring privileges

To manage and create response rules, you must be assigned to a role with response rule authoring privileges. To add a response rule to a policy, you must have policy authoring privileges.

See "Policy authoring privileges" on page 290.

For business reasons, you may want to grant response rule authoring and policy authoring privileges to the same role. Or, you may want to keep these roles separate.

See "About recommended roles for your organization" on page 88.

If you log on to the system as a user without response rule authoring privileges, the Manage > Policies > Response Rules screen is not available.

See "About role-based access control" on page 84.

#### Implementing response rules

You define response rules independent of policies.

See "About response rules" on page 875.

You must have response rule authoring privileges to create and manage response rules.

See "About response rule authoring privileges" on page 885.

Table 36-11 Workflow for implementing policy response rules

Step	Action	Description
Step 1	Review the available response rules.	The Manage > Policies > Response Rules screen displays all configured response rules.
		See "Manage response rules" on page 889.
		The solution pack for your system provides configured response rules. You can use these response rules in your policies as they exist, or you can modify them.
		See "Solution packs" on page 287.
Step 2	Decide the type of response rule to implement: Smart, Automated, both.	Decide the type of response rules based on your business requirements.
		See "About response rule execution types" on page 880.
Step 3	Determine the type of actions you want to	See "About response rule conditions" on page 882.
	implement and any triggering conditions.	See "About response rule actions" on page 875.
· ·	Understand the order of precedence among response rule actions of different and the	See "About response rule action execution priority" on page 883.
	same types.	See "Modifying response rule ordering" on page 895.

Step Action Description Step 5 Integrate the Enforce Server with an external Some response rules may require integration with external system (if required for the response rule). systems. These may include: A SIEM system for the Log to a Syslog Server response An SMTP email server for the Send Email Notification response rule A Web proxy host for Network Prevent for Web response An MTA for Network Prevent for Email response rules. Step 6 Add a new response rule. See "Adding a new response rule" on page 890. Step 7 Configure response rules. See "Configuring response rules" on page 891. Step 8 Configure one or more response rule See "Configuring response rule conditions" on page 892. conditions (optional). Step 9 Configure one or more response rule actions You must define at least one action for a valid response rule. (required). See "Configuring response rule actions" on page 893. The action executes when a policy violation is reported or when a response rule condition is matched. Step 10 Add response rules to policies. You must have policy authoring privileges to add response rules to policies. See "Adding an automated response rule to a policy" on page 350.

Table 36-11 Workflow for implementing policy response rules (continued)

#### Response rule best practices

When implementing response rules, consider the following:

- Response rules are not required for policy execution. In general it is best to implement and fine-tune your policy rules and exceptions before you implement response rules. Once you achieve the desired policy detection results, you can then implement and refine response rules.
- Response rules require at lease one rule action; a condition is optional. If you do not implement a condition, the action always executes when an incident is

reported. If you configure more than one response rule condition, all conditions must match for the response rule action to trigger.

See "About response rule actions" on page 875.

- Response rule conditions are derived from policy rules. Understand the type of rule and exception conditions that the policy implements when you configure response rule conditions. The system evaluates the response rule condition based on how the policy rule counts matches. See "Policy matching conditions" on page 300.
- The system displays only the response rule name for policy authors to select when they add response rules to policies. Be sure to provide a descriptive name that helps policy authors identify the purpose of the response rule. See "Configuring policies" on page 326.
- You cannot combine an Endpoint Prevent: Notify or Endpoint Prevent: Block response rule action with EDM, IDM, or DGM detection methods. If you do, the system displays a warning for the policy that it is misconfigured. See "Manage and add policies" on page 345.
- If you combine multiple response rules in a single policy, make sure that you understand the order of precedence among response rules. See "About response rule action execution priority" on page 883.
- Use Smart Response rules only where it is appropriate for human intervention. See "About configuring Smart Response rules" on page 892.

# Configuring and managing response rules

This chapter includes the following topics:

- Manage response rules
- Adding a new response rule
- Configuring response rules
- About configuring Smart Response rules
- Configuring response rule conditions
- Configuring response rule actions
- Modifying response rule ordering
- About removing response rules

#### Manage response rules

The **Manage > Policies > Response Rules** screen is the home page for managing response rules, and the starting point for adding new ones.

See "About response rules" on page 875.

You must have response rule authoring privileges to manage and add response rules.

See "About response rule authoring privileges" on page 885.

Action	Description
Add Response Rule	Click Add Response Rule to define a new response rule.
	See "Adding a new response rule" on page 890.
Modify Response Rule Order	Click <b>Modify Response Rule Order</b> to modify the response rule order of precedence.  See "Modifying response rule ordering" on page 895.
Edit an existing response rule	Click the response rule to modify it.  See "Configuring response rules" on page 891.
Delete an existing response rule	Click the <b>red X</b> icon next to the far right of the response rule to delete it.  You must confirm the operation before deletion occurs.  See "About removing response rules" on page 896.
Refresh the list	Click the refresh arrow icon at the upper right of the <b>Response Rules</b> screen to fetch the latest status of the rule.

**Table 37-2** Response Rules screen display

Display column	Description
Order The <b>Order</b> of precedence when more than one response rule is configur	
	See "Modifying response rule ordering" on page 895.
Rule	The <b>Name</b> of the response rule.
	See "Configuring response rules" on page 891.
Actions	The type of <b>Action</b> the response rule can take to respond to an incident (required).
	See "Configuring response rule actions" on page 893.
Conditions	The <b>Condition</b> that triggers the response rule (if any).
	See "Configuring response rule conditions" on page 892.

See "Implementing response rules" on page 886.

## Adding a new response rule

Add a new response rule from the Manage > Policies > Response Rules > New Response Rule screen.

See "About response rules" on page 875.

#### To add a new response rule

Click Add Response Rule at the Manage > Policies > Response Rules screen.

See "Manage response rules" on page 889.

2 At the **New Response Rule** screen, select one of the following options:

#### Automated Response

The system automatically executes the response action as the server evaluates incidents (default option).

See "About Automated Response rules" on page 881.

#### Smart Response

An authorized user executes the response action from the **Incident Snapshot** screen in the Enforce Server administration console. See "About Smart Response rules" on page 881.

3 Click **Next** to configure the response rule.

See "Configuring response rules" on page 891.

See "Implementing response rules" on page 886.

#### Configuring response rules

You configure response rules at the Manage > Policies > Response Rules > Configure Response Rule screen.

See "About response rules" on page 875.

#### To configure a response rule

Add a new response rule, or modify an existing one.

See "Adding a new response rule" on page 890.

See "Manage response rules" on page 889.

- 2 Enter a response Rule Name and Description.
- 3 Optionally, define one or more **Conditions** to dictate when the response rule executes.

See "Configuring response rule conditions" on page 892.

If no condition is declared, the response rule action always executes when there is a match (assuming that the detection rule is set the same).

Skip this step if you selected the **Smart Response** rule option.

See "About configuring Smart Response rules" on page 892.

Select and configure one or more **Actions**. You must define at least one action.

See "Configuring response rule actions" on page 893.

5 Click **Save** to save the response rule definition.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## **About configuring Smart Response rules**

When implementing Smart Response rules, consider the following:

- Smart Response rules are best suited for the incidents that warrant user review to determine if any response action is required.
  - If you do not want user involvement in triggering a response rule action, use Automated Response rules instead.
- You cannot configure any triggering conditions with Smart Response rules. Authorized users decide when a detection incident warrants a response.
- You are limited in the actions you can take with Smart Response rules (note, log, email, status).

If you need to block or modify an action, use Automated Response rules.

See "About Smart Response rules" on page 881.

See "Implementing response rules" on page 886.

#### **Configuring response rule conditions**

You can add one or more conditions to a response rule. An incident must meet all response rule conditions before the system executes any response rule actions.

See "About response rule conditions" on page 882.

#### To configure a response rule condition

- 1 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- Click **Add Condition** to add a new condition.

Conditions are optional and based on detection rule matches. Each type of response rule condition performs a different function.

See "About response rule conditions" on page 882.

3 Choose the condition type from the Conditions list.

See Table 36-9 on page 883.

For example, select the condition Incident Match Count and Is Greater Than and enter 15 in the textbox. This condition triggers the response rule action after 15 policy violation matches.

- To add another condition, click **Add Condition** and repeat the process.
  - If all conditions do not match, no action is taken.
- 5 Click **Save** to save the condition.
  - Click **Cancel** to not save the condition and return to the previous screen.
  - Click the **red X** icon beside the condition to delete it from the response rule.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

#### Configuring response rule actions

You must configure at least one action for the response rule to be valid. You can configure multiple response rule actions. Each action is evaluated independently.

See "Implementing response rules" on page 886.

#### To define a response rule action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Choose an action type from the **Actions** list and click **Add Action**.
  - For example, add the All: Add Note action to the response rule. This action lets the remediator annotate the incident.
- 3 Configure the action type by specifying the expected parameters for the chosen action type.
  - See Table 37-3 on page 894.
- Repeat these steps for each action you want to add.
  - If you add additional actions, consider the execution order and possible modification of similar types.
  - See "Modifying response rule ordering" on page 895.
- 5 Click **Save** to save the response rule.
  - See "Manage response rules" on page 889.

**Table 37-3** Configure a response rule action

Incident type	Response rule	Description
All	Add Note	See "Configuring the Add Note action" on page 906.
All	Limit Incident Data Retention	See "Configuring the Limit Incident Data Retention action" on page 906.
All	Log to a Syslog Server	See "Configuring the Log to a Syslog Server action" on page 909.
All	Send Email Notification	See "Configuring the Send Email Notification action" on page 910.
All	Server FlexResponse	See "Configuring the Server FlexResponse action" on page 912.
All	Set Attribute	See "Configuring the Set Attribute action" on page 913.
All	Set Status	See "Configuring the Set Status action" on page 914.
Classification	Classify Enterprise Vault Content	See "Configuring the Classify Enterprise Vault Content response action" on page 915.
Endpoint	FlexResponse	See "Configuring the Endpoint: FlexResponse action" on page 919.
Endpoint Discover	Quarantine File	See "Configuring the Endpoint Discover: Quarantine File action" on page 920.
Endpoint Prevent	Block	See "Configuring the Endpoint Prevent: Block action" on page 922.
Endpoint Prevent	Notify	See "Configuring the Endpoint Prevent: Notify action" on page 924.
Endpoint Prevent	User Cancel	See "Configuring the Endpoint Prevent: User Cancel action" on page 928.
Network and Mobile Prevent for Web	Block FTP Request	See "Configuring the Network and Mobile Prevent for Web: Block FTP Request action" on page 931.
Network and Mobile Prevent for Web	Block HTTP/S	See "Configuring the Network and Mobile Prevent for Web: Block HTTP/S action" on page 931.
Network Prevent for Email	Block SMTP Message	See "Configuring the Network Prevent: Block SMTP Message action" on page 933.
Network Prevent for Email	Modify SMTP Message	See "Configuring the Network Prevent: Modify SMTP Message action" on page 934.
Network and Mobile Prevent for Web	Remove HTTP/S Content	See "Configuring the Network and Mobile Prevent for Web: Remove HTTP/S Content action" on page 935.

Incident type	Response rule	Description
Network Protect	Copy File	See "Configuring the Network Protect: Copy File action" on page 937.
Network Protect	Quarantine File	See "Configuring the Network Protect: Quarantine File action" on page 937.

**Table 37-3** Configure a response rule action (continued)

See "Implementing response rules" on page 886.

#### Modifying response rule ordering

You cannot change the system-defined execution priority for different types of response rule actions. But, you can modify the order of execution for response rule actions of the same type with conflicting instructions.

See "About response rule action execution priority" on page 883.

For example, consider a scenario where you include two response rules in a policy. Each response rule implements a Limit Incident Data Retention action. One action discards all attachments and the other action discards only those attachments that are not violations. In this case, when the policy is violated, the detection server looks to the response rule order priority to determine which action takes precedence. This type of ordering is configurable.

#### To modify response rule action ordering

- Navigate to the **Manage > Policies > Response Rules** screen.
  - See "Manage response rules" on page 889.
- 2 Note the **Order** column and number beside each configured response rule.
  - By default the system sorts the list of response rules by the **Order** column in descending order from highest priority (1) to lowest. Initially the system orders the response rules in the order they are created. You can modify this order.
- 3 To enable modification mode, click **Modify Response Rule Order**.
  - The **Order** column now displays a drop-down menu for each response rule.
- To modify the ordering, for each response rule you want to reorder, select the desired order priority from the drop-down menu.
  - For example, for a response rule with order priority of 2, you can modify it to be 1 (highest priority).
  - Modifying an order number moves that response rule to its modified position in the list and updates all other response rules.

- 5 Click **Save** to save the modifications to the response rule ordering.
- Repeat these steps as necessary to achieve the desired results.

See "Implementing response rules" on page 886.

#### **About removing response rules**

You can delete response rules at the Manage > Policies > Response Rules screen.

See "Manage response rules" on page 889.

When deleting a response rule, consider the following:

- A user must have response rule authoring privileges to delete an existing response rule.
- A response rule author cannot delete an existing response rule while another user modifies it.
- A response rule author cannot delete a response rule if a policy declares that response rule. In this case you must remove the response rule from all policies that declare the response rule before you can delete it.

## Chapter

## Response rule conditions

This chapter includes the following topics:

- Configuring the Endpoint Location response condition
- Configuring the Endpoint Device response condition
- Configuring the Incident Type response condition
- Configuring the Incident Match Count response condition
- Configuring the Protocol or Endpoint Monitoring response condition
- Configuring the Severity response condition

#### Configuring the Endpoint Location response condition

The Endpoint Location condition triggers response rule action based on the connection status of the DLP Agent when an endpoint policy is violated.

See "About response rule conditions" on page 882.

**Note:** This condition is specific to endpoint incidents. You should not implement this condition for Network or Discover incidents. If you do the response rule action does not to execute.

#### To configure the Endpoint Location condition

- 1 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Select the **Endpoint Location** condition from the **Conditions** list.
  - See "Configuring response rule conditions" on page 892.
- 3 Select the endpoint location requirements to trigger actions.
  - See Table 38-1 on page 898.

Table 38-1 **Endpoint Location condition options** 

Qualifier	Condition	Description
Is Any Of	Off the corporate network	This combination triggers a response rule action if an incident occurs when the endpoint is off the corporate network.
Is None Of	Off the corporate network	This combination does not trigger a response rule action if an incident occurs when the endpoint is off the corporate network.
Is Any Of	On the corporate network	This combination triggers a response rule action if an incident occurs when the endpoint is on the corporate network.
Is None Of	On the corporate network	This combination does not trigger a response rule action if an incident occurs when the endpoint is on the corporate network.

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

#### Configuring the Endpoint Device response condition

The Endpoint Device condition triggers response rule action when an incident is detected from one or more configured endpoint devices.

See "About response rule conditions" on page 882.

You configure endpoint devices at the System > Agents > Endpoint Devices screen.

See "About endpoint device detection" on page 634.

Note: This condition is specific to endpoint incidents. You should not implement this condition for Network or Discover incidents. If you do the response rule action does not to execute.

#### To configure the Endpoint Device response condition

Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

2 Select the **Endpoint Device** condition from the **Conditions** list.

See "Configuring response rule conditions" on page 892.

3 Select to detect or except specific endpoint devices.

See Table 38-2 on page 899.

**Table 38-2 Endpoint Device condition parameters** 

Qualifier	Condition	Description
Is Any Of	Configured device	Triggers a response rule action when an incident is detected on a configured endpoint device.
Is None Of	Configured device	Does not trigger (excludes from executing) a response rule action when an incident is detected on a configured endpoint device.

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

#### Configuring the Incident Type response condition

The Incident Type condition triggers a response rule action based on the type of detection server that reports the incident.

See "About response rule conditions" on page 882.

#### To configure the Incident Type condition

Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

2 Choose the **Incident Type** condition from the **Conditions** list.

See "Configuring response rule conditions" on page 892.

Select one or more incident types.

Use the Ctrl key to select multiple types.

See Table 38-3 on page 900.

Table 56 5		
Parameter	Server	Description
Is Any Of	Classification	Triggers a response rule action for any incident that the Classification Server detects.
Is None Of		Does not trigger a response rule action for any incident that the Classification Server detects.
Is Any Of	Discover	Triggers a response rule action for any incident that Network Discover detects.
Is None Of		Does not trigger a response rule action for any incident that Network Discover detects.
Is Any Of	Endpoint	Triggers a response rule action for any incident that Endpoint Prevent detects.
Is None Of		Does not trigger a response rule action for any incident that Endpoint Prevent detects.
Is Any Of	Network or	Triggers a response rule action for any incident that Network Prevent detects.
Is None Of	Mobile	Does not trigger a response rule action for any incident that Network Prevent

**Table 38-3** Incident Type condition parameters

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

detects.

#### **Configuring the Incident Match Count response** condition

The Incident Match Count condition triggers a response rule action based on the number of policy violations reported.

See "About response rule conditions" on page 882.

### To configure the Incident Match Count condition

Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

Choose the **Incident Match Count** condition from the **Conditions** list.

See "Configuring response rule conditions" on page 892.

In the text field, enter a numeric value that indicates the threshold above which you want the response rule to trigger.

For example, if you enter 15 the response rule triggers after 15 policy violations have been detected.

See Table 38-4 on page 901.

Table 38-4 **Incident Match Count condition options** 

Parameter	Input	Description
Is Greater Than	User-specified number	Triggers a response rule action if the threshold number of incidents is eclipsed.
Is Greater Than or Equals	User-specified number	Triggers a response rule action if the threshold number of incidents is met or eclipsed.
Is Between	User-specified pair of numbers	Triggers a response rule action when the number of incidents is between the range of numbers specified.
Is Less Than	User-specified number	Triggers a response rule action if the number of incidents is less than the specified number.
ls Less Than or Equals	User-specified number	Triggers a response rule action when the number of incidents is equal to or less than the specified number.

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

## Configuring the Protocol or Endpoint Monitoring response condition

The Protocol or Endpoint Monitoring condition triggers action based on the protocol or the endpoint destination, device, or application where the policy violation occurred.

See "About response rule conditions" on page 882.

### To configure the Protocol or Endpoint Monitoring condition

1 Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

2 Choose the **Protocol or Endpoint Monitoring** condition from the **Conditions** 

See "Configuring response rule conditions" on page 892.

3 Use the ctrl key to select multiple, or use the Shift key to select a range.

See Table 38-5 on page 902.

The system lists any additional network protocols that you configure at the System > Settings > Protocols screen.

Table 38-5 Protocol or Endpoint Destination condition options

Qualifier	Condition	Description
Is Any Of	Endpoint Application File Access	Triggers an action if an endpoint application file has been accessed.
Is None Of		Does not trigger action if an endpoint application file has been accessed.
Is Any Of	Frade sint CD/D\/D	Triggers an action if an endpoint CD/DVD has been written to.
Is None Of	Endpoint CD/DVD	Does not trigger action if an endpoint CD/DVD has been written to.
Is Any Of	Endpoint Clipboard	Triggers an action if the endpoint clipboard has been copied to.
Is None Of	- спаронн спробага	Does not trigger action if the endpoint clipboard has been copied to.
Is Any Of	Endpoint Copy to Network Share	Triggers an action if sensitive information is copied to or from a network share.
Is None Of		Does not trigger action if sensitive information is copied to or from a network share.
Is Any Of		Triggers an action if sensitive files are discovered on the local drive.
Is None Of	Endpoint Local Drive	Does not trigger action if sensitive files are discovered on the local drive.
Is Any Of	- Endpoint Printer/Fax	Triggers an action if an endpoint printer or fax has been sent to.
Is None Of		Does not trigger action if an endpoint printer or fax has been sent to.

Table 36-3 Protocol of Endpoint Destination condition options (continued)		
Qualifier	Condition	Description
Is Any Of	Endpoint Removable Storage Device	Triggers an action if sensitive data is copied to a removable storage device.
Is None Of		Does not trigger action if sensitive data is copied to a removable storage device.
Is Any Of	FTP	Triggers an action if sensitive data is copied through FTP.
Is None Of		Does not trigger action if sensitive data is copied through FTP.
Is Any Of	HTTP	Triggers an action if sensitive data is sent through HTTP.
Is None Of		Does not trigger action if sensitive data is sent through HTTP.
Is Any Of	- HTTPS	Triggers an action if sensitive data is sent through HTTPS.
Is None Of		Does not trigger action if sensitive data is sent through HTTPS.
Is Any Of	IM:AIM	Triggers an action if sensitive data is sent through AIM.
Is None Of	IIVI.AIIVI	Does not trigger action if sensitive data is sent through AIM.
Is Any Of	IM:MSN	Triggers an action if sensitive data is sent through MSN.
Is None Of	- IIVI.IVISIN	Does not trigger action if sensitive data is sent through MSN.
Is Any Of	IM:Yahoo	Triggers an action if sensitive data is sent through Yahoo IM.
Is None Of	IIVI. Falloo	Does not trigger action if sensitive data is sent through Yahoo IM.
Is Any Of	NNTP	Triggers an action if sensitive data is sent through NNTP.
Is None Of	INNIP	Does not trigger action if sensitive data is sent through NNTP.
Is Any Of	SMTP	Triggers an action if sensitive data is sent through SMTP.
Is None Of	- OWITI-	Does not trigger action if sensitive data is sent through SMTP.

**Table 38-5** Protocol or Endpoint Destination condition options (continued)

See "Manage response rules" on page 889.

## **Configuring the Severity response condition**

The Severity condition triggers a response rule action based on the severity of the policy rule violation.

See "About response rule conditions" on page 882.

### To configure the Severity condition

- 1 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Select the **Severity** condition from the **Conditions** list.
  - See "Configuring response rule conditions" on page 892.
- 3 Select one or more severity levels.

Use the Ctrl key to select multiple; use the Shift key to select a range.

See Table 38-6 on page 904.

Table 38-6 Severity condition matches

Parameter	Severity	Description
Is Any Of	High	Triggers a response rule action when a detection rule with severity set to high is matched.
Is None Of	High	Does not trigger a response rule action when a detection rule with severity set to high is matched.
Is Any Of	Medium	Triggers a response rule action when a detection rule with severity set to medium is matched.
Is None Of	Medium	Does not trigger a response rule action when a detection rule with severity set to medium is matched.
Is Any Of	Low	Triggers a response rule action when a detection rule with severity set to low is matched.
Is None Of	Low	Does not trigger a response rule action when a detection rule with severity set to low is matched.
Is Any Of	Info	Triggers a response rule action when a detection rule with severity set to info is matched.
Is None Of	Info	Does not trigger a response rule action when a detection rule with severity set to info is matched.

See "Implementing response rules" on page 886.

See "Manage response rules" on page 889.

# Response rule actions

### This chapter includes the following topics:

- Configuring the Add Note action
- Configuring the Limit Incident Data Retention action
- Configuring the Log to a Syslog Server action
- Configuring the Send Email Notification action
- Configuring the Server FlexResponse action
- Configuring the Set Attribute action
- Configuring the Set Status action
- Configuring the Classify Enterprise Vault Content response action
- Configuring the Endpoint: FlexResponse action
- Configuring the Endpoint Discover: Quarantine File action
- Configuring the Endpoint Prevent: Block action
- Configuring the Endpoint Prevent: Notify action
- Configuring the Endpoint Prevent: User Cancel action
- Configuring the Network and Mobile Prevent for Web: Block FTP Request action
- Configuring the Network and Mobile Prevent for Web: Block HTTP/S action
- Configuring the Network Prevent: Block SMTP Message action
- Configuring the Network Prevent: Modify SMTP Message action
- Configuring the Network and Mobile Prevent for Web: Remove HTTP/S Content action

- Configuring the Network Protect: Copy File action
- Configuring the Network Protect: Quarantine File action

## Configuring the Add Note action

The Add Note response rule action lets an incident responder enter a note about a particular incident. For example, if a policy violation occurs, the system presents the incident responder with a Note dialog that the responder can annotate.

See "About response rule actions" on page 875.

The Add Note response rule action is available for all types of detection servers.

See "Response rules for all detection servers" on page 876.

### To configure the Add Note action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the All: Add Note action type from the Actions list.

The system displays a **Note** field. Generally you leave the field blank and allow remediators to add comments when they evaluate incidents. However, you can add comments at this level of configuration as well.

- See "Configuring response rule actions" on page 893.
- 3 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## Configuring the Limit Incident Data Retention action

The Limit Incident Data Retention response rule action lets you modify the default incident data retention behavior of the detection server.

See "About response rule actions" on page 875.

This response rule is available for all types of detection servers.

See "Response rules for all detection servers" on page 876.

### To configure incident data retention

1 Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

2 Add the action type All: Limit Incident Data Retention from the Actions list.

See "Configuring response rule actions" on page 893.

3 Choose to retain Endpoint Incident data by selecting this option.

By default, the agent discards the original message and any attachments for endpoint incidents.

See "Retaining data for endpoint incidents" on page 907.

Choose to discard Network Incident data by selecting this option.

By default, the system retains the original message and any attachments for network incidents.

See "Discarding data for network incidents" on page 908.

5 Click **Save** to save the response rule configuration.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## Retaining data for endpoint incidents

By default, the system discards original messages (including files and attachments) for endpoint incidents. You can implement the Limit Incident Data Retention response rule action to override this default behavior and retain original messages for endpoint incidents.

Note: Limit Incident Data Retention does not apply to Endpoint Print or Clipboard incidents.

See "Configuring the Limit Incident Data Retention action" on page 906.

Table 39-1 Retaining data for endpoint incidents

Parameter	Description
All Endpoint Incidents (including Endpoint Discover incidents)	Check this option to retain the original message and file attachments for Endpoint Prevent incidents and incidents Endpoint Discover captures using an endpoint target.

If you combine a server-side detection rule (EDM/IDM/DGM) with a Limit Incident Data Retention response rule action on the endpoint, consider the network bandwidth implications. When an Endpoint Agent sends content to an Endpoint Server for analysis, it sends text or binary data according to detection requirements. If possible, Symantec DLP Agents send text to reduce bandwidth use. When you retain the original messages for endpoint incidents, in every case the system requires agents to send binary data to the Endpoint Server. As such, make sure that your network can handle the increased traffic between Endpoint Agents and Endpoint Servers without degrading performance.

See "Two-tier detection for DLP Agents" on page 309.

Consider the system behavior for any policies that combine an agent-side detection rule (any DCM rule, such as a keyword rule). If you implement the Limit Incident Data Retention response rule action, the increased use bandwidth depends on the number of incidents the detection engine matches. For such policies, the Endpoint Agent does not send all original files to the Endpoint Server, but only those associated with confirmed incidents. If there are not many incidents, the effect is small.

### Discarding data for network incidents

For network incidents, by default the detection server retains the original message and any attachments that trigger an incident.

You can implement the Limit Incident Data Retention response rule action to override the default behavior and discard original messages and some or all attachments.

See "Configuring the Limit Incident Data Retention action" on page 906.

Note: The default data retention behavior for network incidents applies to Network Prevent for Web and Network Prevent for Email incidents. The default behavior does not apply to Network Discover incidents. For Network Discover incidents, the system provides a link in the **Incident Snapshot** that points to the offending file at its original location. Incident data retention for Network Discover is not configurable.

**Table 39-2** Discarding data from network incidents

Parameter	Description
Discard Original	Check this option to discard the original message.
Message	Use this configuration to save disk space when you are only interested in statistical data.

-		
Parameter	Description	
Discard Attachment	nent Select All to discard all message attachments.	
	Select <b>Attachments with no Violations</b> to save only relevant message attachments, that is, those that trigger a policy violation.	
	<b>Note:</b> You must select something other than <b>None</b> for this action option. If you leave <b>None</b> selected and do not check the box next to <b>Discard Original Message</b> , the action has no effect. Such a configuration duplicates the default incident data retention behavior for network servers.	

**Table 39-2** Discarding data from network incidents (continued)

## Configuring the Log to a Syslog Server action

The Log to a Syslog Server response rule action logs the incident to a syslog server. These logs can be useful if you use a Security Information and Events Management (SIEM) system.

See "About response rule actions" on page 875.

This response rule action is available for all types of detection servers.

See "Response rules for all detection servers" on page 876.

Note: You use this response rule in conjunction with a syslog server. See "Enabling a syslog server" on page 144.

### To configure the Log to a Syslog Server response rule action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- Add the Log to a Syslog Server action type from the Actions list.
  - See "Configuring response rule actions" on page 893.
- 3 Enter the **Host** name of the syslog server.
- 4 Edit the **Port** for the syslog server, if necessary.
  - The default port is 514.
- 5 Enter the text of the **Message** to log on the syslog server.
- Select the **Level** to apply to the log message from the drop-down list. The following options are available:
  - 0 Kernel panic

- 1 Needs immediate attention
- 2 Critical condition
- 3 Frror
- 4 Warning
- 5 May need attention
- 6 Informational
- 7- Debugging
- Save the response rule.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## Configuring the Send Email Notification action

The Send Email Notification action sends an email you compose to recipients you specify.

See "About response rule actions" on page 875.

This response rule action is available for all types of detection servers.

See "Response rules for all detection servers" on page 876.

You must integrate the Enforce Server with an SMTP email server to implement this response rule action.

See "Configuring the Enforce Server to send email alerts" on page 146.

### To configure the Send Email Notification response rule action

- Configure a response rule at the **Configure Response Rule** screen. See "Configuring response rules" on page 891.
- Add the All: Send Email Notification action type from the Actions list. 2
  - See "Configuring response rule actions" on page 893.
- Configure the recipient(s), sender, format, incident inclusion, and messages per day.

See Table 39-3 on page 911.

Configure the Notification Content of the email notification: language, subject, body.

See Table 39-4 on page 911.

5 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

Sender and recipient information Table 39-3

Parameter	Description
To: Sender	Select this option to send the email notification to the email sender. This recipient only applies to email message violations.
To: Data Owner	Select this option to send email notification to the data owner that the system identifies by email address in the incident.  See "Discover incident snapshots" on page 991.
To: Other Email Address	This option can include any custom attributes designated as email addresses (such as "manager@email"). For example, if you define a custom attribute that is an email address, or retrieve one via a Lookup Plugin, that address will appear in the "To" field for selection, to the right of "To: Sender" and "To: Data Owner."
	See "Configuring custom attributes" on page 1079.
Custom To	Enter one or more specific email addresses separated by commas.
CC	Enter one or more specific email addresses separated by commas for people you want to copy on the notification.
Custom From	You can specify the sender of the message.
	If this field is blank, the message appears to come from the system email address.
Notification Format	Select either HTML or plain text format.
Include Original Message	Select this option to include the message that generated the incident with the notification email.
Max Per Day	Enter a number to restrict the maximum number of notifications that the system sends in a day.

**Table 39-4** Notification content

Parameter	Description
Language	Select the language for the message from the drop-down menu.

Parameter	Description
Add Language	Click the icon to add multiple language(s) for the message.
	See "About Endpoint Prevent response rules in different locales" on page 1380.
Subject	Enter a subject for the message that indicates what the message is about.
Body	Enter the body of the message.
Insert Variables	You can add one or more variables to the subject or body of the email message by selecting the desired value(s) from the <b>Insert Variables</b> list.
	Variables can be used to include the file name, policy name, recipients, and sender in both the subject and the body of the email message. For example, to include the policy and rules violated, you would insert the following variables.
	A message has violated the following rules in \$POLICY\$: \$RULES\$

Notification content (continued) Table 39-4

## Configuring the Server FlexResponse action

The All: Server FlexResponse action enables you to remediate any incident type using a custom, server-side FlexResponse plug-in. You can configure a Server FlexResponse response action for either automated response rules or smart response rules.

The All: Server FlexResponse action is available only if you have licensed Network Protect and you have deployed one or more Server FlexResponse plug-ins to Symantec Data Loss Prevention.

See "Deploying a Server FlexResponse plug-in" on page 1231.

### To configure a Server FlexResponse action

- Log on to the Enforce Server administration console. 1
- 2 Create a new Response Rule for each custom Server FlexResponse plug-in. Click Manage > Policies > Response Rules.
- 3 Click Add Response Rule.
- Select either Automated Response or Smart Response. Click Next.

- 5 Enter a name for the rule in the **Rule Name** field. (For Smart Response rules, this name appears as the label on the button that incident responders select during remediation.)
- Enter an optional description for the rule in the **Description** field.
- 7 In the Actions (executed in the order shown) menu, select the action All: Server FlexResponse.
- Click Add Action.
- In the FlexResponse Plugin menu, select a deployed Server FlexResponse plug-in to execute with this Response Rule action.

The name that appears in this drop-down menu is the value specified in the display-name property from either the configuration properties file or the plug-in metadata class.

See "Deploying a Server FlexResponse plug-in" on page 1231.

- 10 Click Save.
- 11 Repeat this procedure, adding a Response Rule for any additional Server FlexResponse plug-ins that you have deployed.

## Configuring the Set Attribute action

The Set Attribute response rule action sets the incident status to the specified value.

See "About response rule actions" on page 875.

This response rule action is available for all detection servers.

See "Response rules for all detection servers" on page 876.

The Set Attribute action is based on custom attributes you define at the System > Incident Data > Attributes screen.

See "About custom attributes" on page 1076.

### To configure the Set Attribute action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the All: Sett Attribute action type from the Actions list.
  - See "Configuring response rule actions" on page 893.
- 3 Select the **Attribute** from the drop-down list (if more than one custom attribute is defined).

- Enter an incident status **Value** for the selected custom attribute.
- 5 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## Configuring the Set Status action

The Set Status response rule action sets the incident status to the specified value.

See "About response rule actions" on page 875.

This response rule is available for all detection servers.

See "Response rules for all detection servers" on page 876.

This response rule action is based on the incident Status Values you configure at the System > Incident Data > Attributes screen.

See "About incident status attributes" on page 1069.

### To configure the Set Status response rule action

- Configure a response rule at the Configure Response Rule screen.
  - See "Configuring response rules" on page 891.
- 2 Add the All: Set Status action type from the Actions list.
- See "Configuring response rule actions" on page 893.
- Select the **Status** to assign to the incident from the list.

The following are some example incident statuses you might configure and select from:

- New
- Escalated
- Investigation
- Resolved
- Dismissed
- Click **Save** to save the configuration.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## **Configuring the Classify Enterprise Vault Content** response action

The Classification: Classify Enterprise Vault Content response rule defines the classification result tags that the Classification Server generates for an Exchange message that matches a detection policy. The Classification Server delivers the retention category and classification tag to the Data Classification for Enterprise Vault filter that posted the Exchange message for detection. The classification tag always corresponds to the name of the policy that triggers the response rule action.

Symantec Enterprise Vault for Microsoft Exchange can then use the retention category and classification tag to perform archiving, delete messages, or flag the message for compliance reviews or E-Discovery searches.

See "About implementing detection for Enterprise Vault Classification" on page 620.

To configure the Classify Enterprise Vault Content response rule action

Configure a response rule at the Configure Response Rule screen (Manage > Response Rules).

See "Configuring response rules" on page 891.

2 Add the Classification: Classify Enterprise Vault Content action type from the **Actions** list.

See "Configuring response rule actions" on page 893.

3 Configure the parameters to classify the Enterprise Vault message.

See Table 39-5 on page 915.

Click Save to save the configuration.

See "Manage response rules" on page 889.

**Table 39-5** Classification: Classify Enterprise Vault Content parameters

Parameter	Description
Archive and classify message	Select this option to indicate that Symantec Enterprise Vault should archive the message that matched the detection rule. If you select this option, also use the <b>Assign retention category</b> menu to specify the retention category that Enterprise Vault assigns.

Classification: Classify Enterprise Vault Content parameters **Table 39-5** (continued)

_	(continued)
Parameter	Description
Assign retention category	The <b>Assign retention category</b> menu lists all of the retention categories that you have configured for use with the Data Classification for Enterprise Vault solution. If you configure the response rule to archive a message, also select the appropriate retention category from this menu.
	You should configure the retention category names in this menu to match those categories that are available on Enterprise Vault servers.
	See "Configuring the retention categories that are available for classification" on page 917.
	If you select <b>Do not override retention category</b> , the Classification Server communicates to Enterprise Vault that no retention category has been assigned. Enterprise Vault uses the retention category that is already available with the message and applies it during the archiving process.
	When you configure a response rule, if you do not select the classification type of response rule, then Enterprise Vault cannot receive any response from the Symantec Enterprise Vault Data Classification Services. Enterprise Vault applies the retention category that is already available on the message. If the associated policy was running in test mode, the incident is created, but Enterprise Vault does not receive any response from the Classification Server. Not even test mode logs on Enterprise Vault are updated.
Compliance review	If you configure the response rule to archive the message, you can also select <b>Prioritize messages for compliance review</b> to prioritize the message for review. The Discovery Accelerator and Compliance Accelerator products can use this classification tag to filter messages during searches or audits.
	When you select this option, two additional choices are presented:
	<ul> <li>Include in review—Includes the message in subsequent searches and audits.</li> <li>Exclude from review—Excludes the message from subsequent searches and audits.</li> </ul>
	See the Discovery Accelerator and Compliance Accelerator documentation for more information about searching and auditing messages in Enterprise Vault.

Table 39-5	Classification: Classify Enterprise Vault Content parameters
	(continued)

, ,	
Parameter	Description
Do not archive	Choose this option to indicate that Symantec Enterprise Vault should not archive the message that matched the detection rule.
message	When you select this option, the following choices are presented to specify the way in which Enterprise Vault should discard the message:
	■ Delete message immediately and permanently—Enterprise Vault should delete the message immediately.
	■ Move message to Deleted Items folder—Enterprise Vault should move the message to the Deleted Items folder. The message may be deleted at a later time when the folder is emptied.
	■ Leave message in mailbox—Enterprise Vault should leave the message in the mailbox and mark it as "Do not archive."
	If you select this option but later decide to clear the "Do Not Archive" property on messages, you can do so by setting the <b>ClearDoNotArchive</b> and <b>ClearDoNotJournal</b> registry values on the Enterprise Vault server. See the <i>Enterprise Vault Registry Values</i> manual for instructions. These values permit the Exchange mailbox and Exchange Journaling tasks to archive the messages.
	Note: When you monitor a Journal mailbox, you may see messages marked as "Do not archive" in the journal Inbox and in the Deleted items folder. Messages that are marked as "Do not archive" are not automatically re-located. You can manually move the messages into the deleted items folder.

See "About response rule actions" on page 875.

See "Implementing response rules" on page 886.

### Configuring the retention categories that are available for classification

The Classification: Classify Enterprise Vault Content response rule defines the classification result tags that a Classification Server generates for an Exchange message that matches a detection policy. If you configure this response rule to perform the **Archive and classify message** action, you also specify the retention category that Enterprise Vault should apply to the archived message. The list of available retention categories that is shown in the Enforce Server administration console is defined using a configuration file, RetentionCategories.config.

See "Configuring the Classify Enterprise Vault Content response action" on page 915.

When you first install the Data Classification Services solution, you must create a RetentionCategories.config file to include the retention categories that are available in Enterprise Vault servers. If you change the retention categories that are available in an Enterprise Vault deployment, you should also manually change the available categories that are defined in RetentionCategories.config.

Note: The RetentionCategories.config file supports UTF-8 character encoding without byte order markers (BOM).

### To configure the retention categories that are available for classification

- One each Enterprise Vault server, run the ExportRetentionCategories.exe command-line utility that is installed in the Enterprise Vault program folder. (To display usage instructions, execute the utility without supplying any command-line options). You must open the command-line utility from a user with administrator privileges
- 2 Follow the on-screen instructions to generate a file that lists the retention categories available in the Enterprise Vault server. The following retention categories are always excluded from the file:
  - The retention categories for managed folders.
  - For English deployments, any retention category with the name <Do not</li> override retention category> does not apply a new retention category. Instead, a retention category that is already available for the message is applied during the archiving process.

Keep in mind that hidden retention categories are included in the resulting file.

- 3 Repeat steps 1 and 2 for each Enterprise Vault server in your deployment.
- 4 If you generated files for multiple Enterprise Vault servers, use a text editor to merge the contents of each file into a single file.
- 5 Rename the file that contains all retention categories to RetentionCategories.config.
- Log on to the Enforce Server computer using Administrator or superuser privileges.

- Copy the RetentionCategories.config file that you created to the config subdirectory of the Symantec Data Loss Prevention product installation directory. The default directory is c:\SymantecDLP\Protect\config.
- Restart the Enforce Server to apply the changes. 8

See "Server controls" on page 178.

See the Symantec Data Loss Prevention Administration Guide for information about starting and stopping Symantec Data Loss Prevention services.

## Configuring the Endpoint: FlexResponse action

The Endpoint: FlexResponse response rule action lets you implement one or more custom responses you have developed using the FlexResponse API.

See "About Endpoint FlexResponse" on page 1512.

This response rule is available for Endpoint Discover.

Note: This feature is not yet available for agents running on Mac endpoints.

See "Response rules for endpoint detection" on page 877.

To configure the Endpoint: FlexResponse response rule action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the **Endpoint: FlexResponse** action type from the **Actions** list.
  - See "Configuring response rule actions" on page 893.
- 3 Enter the FlexResponse plug-in **Name** and configure its **Parameters**.
  - See Table 39-6 on page 919.
- Click **Save** to save the configuration.
  - See "Manage response rules" on page 889.

**Table 39-6** Endpoint: FlexResponse response rule action parameters

Parameter	Description
FlexResponse Python Plugin	Enter the script module name with packages separated by a period (.).
Plugin parameters	Click Add Parameter to add one or more parameters to the script.
	Enter the <b>Key/Value</b> pair for each parameter.

Parameter	Description
Credentials	You can add credentials for accessing the plugin.
	You can add and store credentials at the <b>System &gt; Settings &gt; Credentials</b> screen.
	See "About the credential store" on page 131.

**Table 39-6** Endpoint: FlexResponse response rule action parameters (continued)

See "Implementing response rules" on page 886.

## Configuring the Endpoint Discover: Quarantine File action

The Endpoint Discover: Quarantine File response rule action removes a file containing sensitive information from a non-secure location and places it in a secure location.

See "About Endpoint Quarantine" on page 1388.

This response rule action is specific to Endpoint Discover incidents. This response rule is not applicable to two-tiered detection methods requiring a Data Profile.

See "Setting up and configuring Endpoint Discover" on page 1389.

If you use multiple endpoint response rules in a single policy, make sure that you understand the order of precedence for such rules.

See "About response rule action execution priority" on page 883.

**Note:** This feature is not available for agents running on Mac endpoints.

#### To configure the Endpoint Discover: Quarantine File response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen. See "Configuring response rules" on page 891.
- Add the Endpoint Discover: Quarantine File action type from the Actions list.
  - See "Configuring response rule actions" on page 893.
- 3 Enter the Quarantine Path and the Marker File settings.
  - See Table 39-7 on page 921.
- Click **Save** to save the configuration.
  - See "Manage response rules" on page 889.

Endpoint Discover: Quarantine File response rule action parameters **Table 39-7** 

Parameter	Description
Quarantine Path	Enter the path to the secured location where you want files to be placed. The secure location can either be on the local drive of the endpoint, or can be on a remote file share. EFS folders can also be used as the quarantine location.
Access Mode	If your secure location is on a remote file share, you must select how the Symantec DLP Agent accesses that file share.
	Select one of the following credential access types:
	<ul><li>Anonymous Access</li><li>Use Saved Credentials</li></ul>
	In anonymous mode, the Symantec DLP Agent runs as LocalSystem user to move the confidential file. You can use anonymous mode to move files to a secure location on a local drive or to remote share if it allows anonymous access.
	Note: EFS folders cannot accept anonymous users.
	A specified credential lets the Symantec DLP Agent impersonate the specified user to access the secure location. The credentials must be in the following format:
	domain\user
	You must enter the specified credentials you want to use through the System Credentials page.
	See "Configuring endpoint credentials" on page 132.
Marker File	Select the <b>Leave marker in place of the remediated file</b> check box to create a placeholder file that replaces the confidential file.
Marker Text	Specify the text to appear in the marker file. If you selected the option to leave the marker file in place of the remediated file, you can use variables in the marker text.
	To specify the marker text, select the variable from the <b>Insert Variable</b> list.
	For example, for Marker Text you might enter:
	A message has violated the following rules in \$POLICY\$: \$RULES
	Or, you might enter:
	\$FILE_NAME\$ has been moved to \$QUARANTINE_PARENT_PATH\$

See "About response rule actions" on page 875.

See "Response rules for endpoint detection" on page 877.

## Configuring the Endpoint Prevent: Block action

The Endpoint Prevent: Block response rule action blocks the movement of confidential data on the endpoint and optionally displays an on-screen notification to the endpoint user.

See "About response rule actions" on page 875.

This response rule action is specific to Endpoint Prevent incidents. This response rule is not applicable to two-tiered detection methods requiring a Data Profile.

See "Setting up and configuring Endpoint Discover" on page 1389.

If you combine multiple endpoint response rules in a single policy, make sure that you understand the order of precedence for such rules.

See "About response rule action execution priority" on page 883.

**Note:** The block action is not triggered for a copy of sensitive data to a local drive.

### To configure the Endpoint Prevent: Block response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen. See "Configuring response rules" on page 891.
- 2 Add the **Endpoint Prevent: Block** action type from the **Actions** list.
- 3 See "Configuring response rule actions" on page 893.
- Enter the **Endpoint Notification Content** settings.

See Table 39-8 on page 922.

5 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

**Table 39-8** Endpoint Prevent: Block response rule action parameters

Parameter	Configuration
Language	Select the language you want the response rule to execute on. Click <b>Add Language</b> to add more than one language.
	See "About Endpoint Prevent response rules in different locales" on page 1380.
	See "Setting Endpoint Prevent response rules for different locales" on page 1381.

Endpoint Prevent: Block response rule action parameters (continued) **Table 39-8** 

Parameter	Configuration
Display Alert Box with this message	This field is optional for Endpoint Block actions. Select an Endpoint Block action to display an on-screen notification to the endpoint user when the system blocks an attempt to copy confidential data.
	Enter the notification message in the text box. You can add variables to the message by selecting the appropriate value(s) from the <b>Insert Variable</b> box.
	Optionally, you can configure the on-screen notification to include user justifications as well as an option for users to enter their own justification.
	You can also add hyperlinks to refer users to URLs that contain company security information. To add hyperlinks you use standard HTML syntax, tags, and URLs. Tags are case-sensitive. You can include insert hyperlinked text between regular text. For example, you would enter:
	The \$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contains sensitive information. <a href="http://www.company.com">Click here for information</a> . Contact the <a href="mailto:admin@company.com">administrator</a> if you have questions.
Insert Variable	Select the variables to include in the on-screen notification to the endpoint when the system blocks an attempt to copy confidential data.
	You can select variables based on the following types:
	■ Application
	■ Content Name
	Content Type
	Device Type     Policy Names
	Protocol

**Table 39-8** Endpoint Prevent: Block response rule action parameters (continued)

Parameter	Configuration
Allow user to choose explanation	Select this option to display up to four user justifications in the on-screen notification. When the notification appears on the endpoint, the user is required to choose one of the justifications. (If you select <b>Allow user to enter text explanation</b> , the user can enter a justification.) Symantec Data Loss Prevention provides four default justifications, which you can modify or remove as needed.
	Justification:
	<ul> <li>User Education</li> <li>Broken Business Process</li> <li>Manager Approved</li> <li>False positive</li> </ul>
	Each justification entry consists of the following options:
	<ul> <li>Check box         This option indicates whether to include the associated justification in the notification. To remove a justification, clear the check box next to it. To include a justification, select the check box next to it.         Justification         The system label for the justification. This value appears in reports (for ordering and filtering purposes), but the user does not see it. You can select the desired option from the drop-down     </li> </ul>
	list.
	Option Presented to End User The justification text the system displays in the notification. This value appears in reports with the justification label. You can modify the default text as desired.
	To add a new justification, select <b>New Justification</b> from the drop-down list. In the <b>Enter new justification</b> text box that appears, enter the justification name. When you save the rule, Symantec Data Loss Prevention includes it as an option (in alphabetical order) in all <b>Justification</b> drop-down lists.
	<b>Note:</b> You should be selective when adding new justifications. Deleting new justifications is not currently supported.
Allow user to enter text explanation	Select this option to include a text box into which users can enter their own justification.

See "Response rules for endpoint detection" on page 877.

## **Configuring the Endpoint Prevent: Notify action**

The Endpoint Prevent: Notify response rule action displays an on-screen notification to the endpoint user when the user attempts to copy or send a sensitive file. You

can provide a reason for the notification as well as options for the endpoint user to give a justification for the action.

See "About response rule actions" on page 875.

This response rule action is available for Endpoint Prevent.

See "How to implement Endpoint Prevent" on page 1378.

Note: The notify action is not triggered for a copy of sensitive data to a local drive.

### To configure the Endpoint Prevent: Notify action

Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

Add the Endpoint Prevent: Notify action type from the Actions list.

See "Configuring response rule actions" on page 893.

2 Configure the action parameters.

See Table 39-9 on page 925.

3 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

**Table 39-9** Endpoint Prevent: Notify response rule action parameters

Parameter	Description
Language	Select the language you want the response rule to execute on.
	Click Add Language to add more than one language.
	See "About Endpoint Prevent response rules in different locales" on page 1380.
	See "Setting Endpoint Prevent response rules for different locales" on page 1381.

Endpoint Prevent: Notify response rule action parameters **Table 39-9** (continued)

Parameter	Description
Display Alert Box with this message	This field is required for Endpoint Notify actions. Select this option to display an on-screen notification to the endpoint user.
	Enter the notification message in the text box. You can add variables to the message by selecting the appropriate value(s) from the <b>Insert Variable</b> box.
	Optionally, you can configure the on-screen notification to include user justifications as well as the option for users to enter their own justifications.
	You can also add hyperlinks to refer users to URLs that contain company security information. To add hyperlinks you use standard HTML syntax, tags, and URLs. Tags are case-sensitive. You can include insert hyperlinked text between regular text. For example, you would enter:
	The \$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contains sensitive information. <a href="http://www.company.com">Click here for information</a> . Contact the <a href="mailto:admin@company.com">administrator</a> if you have questions.
Insert Variable	Select the variables that you want to include in the on-screen notification to the endpoint user.  You can select variables based on the following types:  Application Content Name Content Type Device Type Policy Names Protocol

Endpoint Prevent: Notify response rule action parameters **Table 39-9** (continued)

Parameter	Description
Allow user to choose explanation	Select this option to display up to four user justifications in the on-screen notification. When the notification appears on the endpoint, the user is required to choose one of the justifications. (If you select <b>Allow user to enter text explanation</b> , the user can enter a justification.) Symantec Data Loss Prevention provides four default justifications, which you can modify or remove as needed.
	Available Justifications:  Broken Business Process False positive Manager Approved User Education
	■ Custom (new justification)  Each justification entry consists of the following options:  ■ Check box
	This option indicates whether to include the associated justification in the notification. To remove a justification, clear the check box next to it. To include a justification, select the check box next to it.  Justification  The system label for the justification. This value appears in reports (for ordering and filtering purposes), but the user does not see it. You can select the desired option from the drop-down
	list.  Option Presented to End User The justification text Symantec Data Loss Prevention displays in the notification. This value appears in reports with the justification label. You can modify the default text as desired.
	To add a new justification, select <b>New Justification</b> from the appropriate drop-down list. In the <b>Enter new justification</b> text box that appears, type the justification name. When you save the rule, the system includes the new justification as an option (in alphabetical order) in all <b>Justification</b> drop-down lists.
	<b>Note:</b> You should be selective in adding new justifications. Deleting new justifications is not currently supported.
Allow user to enter text explanation	Select this option to include a text box into which users can enter their own justification.

See "Response rules for endpoint detection" on page 877.

## Configuring the Endpoint Prevent: User Cancel action

The Endpoint Prevent: User Cancel response rule action displays a time-sensitive notification to the user when a policy is violated.

See "About response rule actions" on page 875.

Users have a limited amount of time to decide to ignore the policy violation or not. If the violation is ignored, the data transfer completes and an incident is created. If the violation is not ignored, the data transfer is stopped and an incident is created. If the user does not make a decision in the allotted time, the data transfer is automatically blocked and an incident is created. You can provide a reason for the notification as well as options for the endpoint user to enter a justification for the action.

This response rule action is available for Endpoint Prevent.

See "How to implement Endpoint Prevent" on page 1378.

### To configure the Endpoint Prevent: User Cancel action

Configure a response rule at the Configure Response Rule screen. 1

See "Configuring response rules" on page 891.

Add the Endpoint Prevent: User Cancel action type from the Actions list.

See "Configuring response rule actions" on page 893.

Configure the **Endpoint Prevent: User Cancel** parameters.

See Table 39-10 on page 928.

3 Click **Save** to save the configuration.

See "Manage response rules" on page 889.

Table 39-10 **Endpoint Prevent: User Cancel parameters** 

Parameter	Description
Language	Select the language you want the response rule to execute on.
	Click <b>Add Language</b> to add more than one language.
	See "About Endpoint Prevent response rules in different locales" on page 1380.
	See "Setting Endpoint Prevent response rules for different locales" on page 1381.
Pre-timeout warning	This field is required to notify users that they have a limited amount of time to respond to the incident.
	Enter the notification message in the text box. You can add variables to the message by selecting the appropriate value(s) from the <b>Insert Variable</b> box.

#### Endpoint Prevent: User Cancel parameters (continued) Table 39-10

Parameter	Description
Post-timeout message	This field notifies users that the amount of time to override the policy has expired. The data transfer was blocked.
	Enter the notification message in the text box. You can add variables to the message by selecting the appropriate value(s) from the <b>Insert Variable</b> box.
Display Alert Box with this message	This field is required for Endpoint User Cancel actions. Select this option to display an on-screen notification to the endpoint user.
	Enter the notification message in the text box. You can add variables to the message by selecting the appropriate value(s) from the <b>Insert Variable</b> box.
	Optionally, you can configure the on-screen notification to include user justifications as well as the option for users to enter their own justifications.
	You can also add hyperlinks to refer users to URLs that contain company security information. To add hyperlinks you use standard HTML syntax, tags, and URLs. Tags are case-sensitive. You can include insert hyperlinked text between regular text. For example, you would enter:
	The \$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contains sensitive information. <a href="http://www.company.com">Click here for information</a> . Contact the <a href="mailto:admin@company.com">administrator</a> if you have questions.
Insert Variable	Select the variables that you want to include in the on-screen notification to the endpoint user.
	You can select variables based on the following types:
	■ Application
	Content Type
	Content Type     Device Type
	■ Policy Name
	■ Protocol
	■ Timeout Counter
	<b>Note:</b> You must use the Timeout Counter variable to display how much time remains before blocking the data transfer.

	Table 39-10	Endpoint Prevent: User Cancel parameters (continued)
Parameter	Description	
Allow user to choose explanation.	the notification appea (If you select <b>Allow us</b> Data Loss Prevention needed. Available Justification	
	<ul> <li>Broken Business I</li> <li>False positive</li> <li>Manager Approve</li> <li>User Education</li> <li>Custom (new justi</li> </ul>	d
	Each justification entr	y consists of the following options:
		tes whether to include the associated justification in the notification. To cition, clear the check box next to it. To include a justification, select the it.
		or the justification. This value appears in reports (for ordering and filtering user does not see it. You can select the desired option from the drop-down
	The justification te	xt Symantec Data Loss Prevention displays in the notification. This value with the justification label. You can modify the default text as desired.
	Enter new justificati	tion, select <b>New Justification</b> from the appropriate drop-down list. In the <b>on</b> text box that appears, type the justification name. When you save the des the new justification as an option (in alphabetical order) in all own lists.
	<b>Note:</b> You should be currently supported.	selective in adding new justifications. Deleting new justifications is not
Allow user to enter text explanation.	Select this option to in	nclude a text box into which users can enter their own justification.

## Configuring the Network and Mobile Prevent for Web: **Block FTP Request action**

The Network and Mobile Prevent for Web: Block FTP Request response rule action blocks any file transfer by FTP on your network or mobile device.

See "About response rule actions" on page 875.

This response rule is available only for Network Prevent for Web integrated with a proxy server or Mobile Prevent for Web integrated with both a VPN server and a proxy server.

See "Configuring Network Prevent for Web Server" on page 1167.

See "Implementing Mobile Prevent for Web" on page 1542.

To configure the Network and Mobile Prevent for Web: Block FTP Request response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the Network and Mobile Prevent for Web: Block FTP Request action type from the Actions list.
  - The Block FTP Request response rule action does not require any further configuration. Once the response rule is deployed to a policy, this action blocks any FTP attempt.
  - See "Configuring response rule actions" on page 893.
- 3 Click Save to save the configuration.

See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

## Configuring the Network and Mobile Prevent for Web: **Block HTTP/S action**

The Network and Mobile Prevent for Web: Block HTTP/S response rule action blocks the transmission of Web content that Network Prevent for Web or Mobile Prevent for Web detects. This action also blocks Web-based email messages and attachments.

See "About response rule actions" on page 875.

This response rule action blocks the transmission of Web content using the Internet Content Adaptation Protocol (ICAP). To implement this response rule action you

must integrate the detection server with a Web proxy server. For Mobile Prevent for Web, you must also integrate with a VPN server.

See "Configuring Network Prevent for Web Server" on page 1167.

See "Implementing Mobile Prevent for Web" on page 1542.

### To configure the Network Prevent: Block HTTP/S response rule action

Integrate Network Prevent for Web or Mobile Prevent for Web with a proxy server and, if necessary, a VPN server.

See "Network Prevent for Web Server—basic configuration" on page 187.

2 Configure a response rule at the **Configure Response Rule** screen.

See "Configuring response rules" on page 891.

Add the Network and Mobile Prevent for Web: Block HTTP/S action type from the Actions list.

See "Configuring response rule actions" on page 893.

4 Edit the Rejection Message, as necessary.

The system presents this message to the user's browser when the action blocks content.

For example, you might include some HTML-coded text to display in a browser.

Note: If the requesting client does not expect an HTML response, the Rejection Message may not be displayed in the client browser. For example, a client expecting an XML response to a Web post may only indicate a Javascript error.

Click **Save** to save the configuration of the response rule.

Certain applications may not provide an adequate response to the Network and Mobile Prevent for Web: Block HTTP/S response action. This behavior has been observed with the Yahoo! Mail application when a detection server blocks a file upload. If a user tries to upload an email attachment and the attachment triggers a Network and Mobile Prevent for Web: Block HTTP/S response action, Yahoo! Mail does not respond or display an error message to indicate that the file is blocked. Instead, Yahoo! Mail appears to continue uploading the selected file, but the upload never completes. The user must manually cancel the upload at some point by pressing Cancel.

Other applications may also exhibit this behavior, depending on how they handle the block request. In these cases a detection server incident is created and the file upload is blocked even though the application provides no such indication.

## Configuring the Network Prevent: Block SMTP Message action

The Network Prevent: Block SMTP Message response rule action blocks SMTP email messages that cause an incident on the Network Prevent (Email) detection server.

See "About response rule actions" on page 875.

This response rule action is only available with Network Prevent for Email.

See "Response rules for Network and Mobile Prevent for Web detection" on page 878.

You must integrate the Network Prevent for Email detection server with a Mail Transfer Agent (MTA) to implement this response rule action. Refer to the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email) for details.

### To configure the Block SMTP Message response rule action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the Network Prevent: Block SMTP Message action type from the Actions list.
  - See "Configuring response rule actions" on page 893.
- Configure the Block SMTP Message action parameters.
  - See Table 39-11 on page 933.
- Click **Save** to save the response rule.
  - See "Manage response rules" on page 889.

Table 39-11 Network Prevent: Block SMTP Message parameters

Parameter	Description
Bounce Message to Sender	Enter the text that you want to appear in the SMTP error that Network Prevent (Email) returns to the MTA. Some MTAs display this text in the message that is bounced to the sender.
	If you leave this field blank, the message does not bounce to the sender but the MTA sends its own message.

Parameter	Description
Redirect Message to this Address	If you want to redirect blocked messages to a particular address (such as the Symantec Data Loss Prevention administrator), enter that address in this field.
	If you leave this field blank, the bounced message goes to the sender only.

Table 39-11 Network Prevent: Block SMTP Message parameters (continued)

## Configuring the Network Prevent: Modify SMTP Message action

The Network Prevent: Modify SMTP Message response rule action lets you modify a sensitive email. For example, you can use this action to change an email subject header to include information about the policy violation type.

See "About response rule actions" on page 875.

This response rule action is only available for Network Prevent for Email.

See "Response rules for Network and Mobile Prevent for Web detection" on page 878.

#### To configure the Network Prevent: Modify SMTP Message action

- Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the **Network Prevent: Modify SMTP Message** action type from the Actions list.
  - See "Configuring response rule actions" on page 893.
- Configure the action parameters.
  - See Table 39-12 on page 935.
- Click **Save** to save the configuration.
  - See "Manage response rules" on page 889.

	Tuble 33 12 Network Prevent. Mounty SWIT Message parameters
Parameter	Description
Subject	Select the type of modification to make to the subject of the message from the following options:  Do not Modify – No text is changed in the subject.  Prepend – New text is added to the beginning of the subject.  Append – New text is added to the end of the subject.  Replace With – New text completely replaces the old subject text.  If the subject text is currently modified, specify the new text.  For example, if you want to prepend "VIOLATION" to the subject of the message, select Prepend and enter VIOLATION in the text field.
Headers	Enter a unique name and a value for each header you want to add to the message (up to three).
Enable Email Quarantine Connect (Requires Symantec Messaging Gateway)	Select this option to enable integration with Symantec Messaging Gateway. When this option is enabled, Symantec Data Loss Prevention adds preconfigured x-headers to the message that inform Symantec Messaging Gateway that the message should be quarantined.  For more information, see the Symantec Data Loss Prevention Email Quarantine Connect FlexResponse Implementation Guide.

Table 39-12 Network Prevent: Modify SMTP Message parameters

## Configuring the Network and Mobile Prevent for Web: Remove HTTP/S Content action

The Network and Mobile Prevent for Web: Remove HTTP/S Content response action removes confidential data that is posted to Web mail sites (such as Gmail), blogs (such as Blogspot), and other sites. This action also removes confidential data that is included in any files that users upload to Web sites or attach to Web mail. This action only applies to HTTP/S POST commands; it does not apply to GET commands.

See "About response rule actions" on page 875.

This response rule action is only available for Network Prevent for Web and Mobile Prevent for Web.

See "Response rules for Network and Mobile Prevent for Web detection" on page 878.

Symantec Data Loss Prevention recognizes Web form fields for selected Web mail, blog, and social networking sites. If Network Prevent for Web or Mobile Prevent for Web cannot remove confidential data for a Web site it recognizes, it creates a system event and performs a configured fallback option.

Note: Symantec Data Loss Prevention removes content for file uploads and, for Network Prevent, Web mail attachments even for those sites that it does not recognize for HTTP content removal.

### To configure the Network and Mobile Prevent for Web: Remove HTTP/S Content action

- 1 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 2 Add the Network and Mobile Prevent for Web: Remove HTTP/S Content action type from the **Actions** list.
  - See "Configuring response rule actions" on page 893.
- **3** Configure the action parameters.
  - See Table 39-13 on page 936.
- 4 Click **Save** to save the configuration.
  - See "Manage response rules" on page 889.

Network and Mobile Prevent for Web: Remove HTTP/S Content Table 39-13 parameters

Field	Description
Removal Message	The message that appears in content (Web postings, Web mail, or files) from which the system has removed confidential information. Only the recipient sees this message.
Fallback option	The action to take if Network Prevent for Web or Mobile Prevent for Web cannot remove confidential information that was detected in an HTTP or HTTPS post.
	The available options are <b>Block</b> (the default) and <b>Allow</b> .
	<b>Note:</b> Symantec Data Loss Prevention removes confidential data in file uploads and, for Network Prevent, Web mail attachments, even for sites in which it does not perform content removal. The <b>Fallback option</b> is taken only in cases where Symantec Data Loss Prevention detects confidential content in a recognized Web form, but it cannot remove the content.
Rejection Message	The message that Network Prevent or Mobile Prevent returns to a client when it blocks an HTTP or HTTPS post. The client Web application may or may not display the rejection message, depending on how the application handles error messages.

See "Implementing response rules" on page 886.

# **Configuring the Network Protect: Copy File action**

The Network Protect: Copy File response rule action copies a sensitive file to the local file system.

See "About response rule actions" on page 875.

This response rule action is only available for Network Discover that is configured for Network Protect.

See "Response rules for Network and Mobile Prevent for Web detection" on page 878.

#### To configure the Network Protect: Copy File response rule action

- Configure a network file share and specify a location to copy files to.
  - See "Configuring Network Protect for file shares" on page 1258.
- 2 Configure a response rule at the **Configure Response Rule** screen.
  - See "Configuring response rules" on page 891.
- 3 Select the **Network Protect: Copy File** action type from the **Actions** list.
  - This action does not require you to configure any parameters.
  - See "Configuring response rule actions" on page 893.
- Click **Save** to save the configuration.
  - See "Manage response rules" on page 889.

See "Implementing response rules" on page 886.

# Configuring the Network Protect: Quarantine File action

The Network Protect: Quarantine File response rule action quarantines a file that the detection server identifies as sensitive or protected.

See "About response rule actions" on page 875.

This response rule action is only available for Network Discover that is configured for Network Protect.

See "Response rules for Network and Mobile Prevent for Web detection" on page 878.

# To configure the Network Protect: Quarantine File response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen See "Configuring response rules" on page 891.
- 2 Add the **Network Protect: Quarantine File** action type from the **Actions** list. See "Configuring response rule actions" on page 893.
- Configure the **Network Protect: Quarantine File** parameters. 3 See Table 39-14 on page 938.
- Click **Save** to save the configuration. See "Manage response rules" on page 889.

Table 39-14 Network Protect: Quarantine File configuration parameters

Parameter	Description
Marker File	Select this option to create a marker text file to replace the original file. This action notifies the user what happened to the file instead of quarantining or deleting the file without any explanation.
	<b>Note:</b> The marker file is the same type and has the same name as the original file, as long as it is a text file. An example of such a file type is Microsoft Word. If the original file is a PDF or image file, the system creates a plain text marker file. The system then gives the file the same name as the original file with .txt appended to the end. For example, if the original file name is accounts.pdf, the marker file name is accounts.pdf.txt.
Marker Text	Specify the text to appear in the marker file. If you selected the option to leave the marker file in place of the remediated file, you can use variables in the marker text.
	To specify marker text, select the variable from the Insert Variable list.
	For example, for Marker Text you might enter:
	A message has violated the following rules in \$POLICY\$: \$RULES
	Or, you might enter:
	\$FILE_NAME\$ has been moved to \$QUARANTINE_PARENT_PATH\$

See "Implementing response rules" on page 886.

Section 6

# Remediating and managing incidents

- Chapter 40. Remediating incidents
- Chapter 41. Remediating Network incidents
- Chapter 42. Remediating Endpoint incidents
- Chapter 43. Remediating Mobile incidents
- Chapter 44. Remediating Discover incidents
- Chapter 45. Working with Classification incidents
- Chapter 46. Managing and reporting incidents
- Chapter 47. Archiving incidents
- Chapter 48. Working with incident data
- Chapter 49. Working with user risk
- Chapter 50. Implementing lookup plug-ins

Chapter 40

# Remediating incidents

This chapter includes the following topics:

- About incident remediation
- Remediating incidents
- Executing Smart response rules
- Incident remediation action commands
- Response action variables
- Monitor and Prevent incident variables.
- Mobile incident variables
- Discover incident variables

# About incident remediation

As incidents occur in your system, individuals in your organization must analyze the incidents, determine why they occurred, identify trends, and remediate the problems.

Symantec Data Loss Prevention provides a rich set of capabilities which can be used to build an effective incident remediation process. Once you are ready to take action, you can use a series of incident commands on the **Incident Snapshot** and **Incident List** pages.

Since the **Incident Snapshot** page displays details about one specific incident, you can select a command to perform an action on the displayed incident.

On the **Incident List** page, you can perform an action on multiple incidents at one time. You can select more than one incident from the list and then choose the desired command.

Table 40-1 describes the options that are involved in incident remediation:

Options involved in incident remediation Table 40-1

Remediation options	Description
Role-based access control	Access to incident information in the Symantec Data Loss Prevention system can be tightly controlled with role-based access control. Roles control which incidents a particular remediator can take action on, as well as what information within that incident is available to the remediator. For example, access control can be used to ensure that a given remediator can act only on incidents originating within a particular business unit. In addition, it might prevent that business unit's staff from ever seeing high-severity incidents, instead routing those incidents to the security department.  See "About role-based access control" on page 84.
Severity level assignment	Incident severity is a measure of the risk that is associated with a particular incident. For example, an email message containing 50 customer records can be considered more severe than a message containing 50 violations of an acceptable use policy. Symantec Data Loss Prevention lets you specify what constitutes a severe incident by configuring it at the policy rule level. Symantec Data Loss Prevention then uses the severity of the incident to drive subsequent responses to the incident. This process lets you prioritize incidents and devote your manual remediation resources to the areas where they are needed most.
Custom attribute lookup	Custom attribute lookup is the process of collecting additional information about the incident from data sources outside of Enforce and the incident itself. For example, a corporate LDAP server can be queried for additional information about the message sender, such as the sender's manager name or business unit.
	See "About using custom attributes" on page 1078.
	For example, you can use custom attributes as input to subsequent automated responses to automatically notify the sender's manager about the policy violation.
	See "Setting the values of custom attributes manually" on page 1080.

Options involved in incident remediation (continued) **Table 40-1** 

Remediation options	Description
Automated incident responses	A powerful feature of the Enforce Server is the ability to automatically respond to incidents as they arise. For example, you can configure the system to respond to a serious incident by blocking the offending communication. You can send an email message to the sender's manager. You can send an alert to a security event management system. You can escalate the incident to the security department. On the other hand, an acceptable use incident might be dispensed with by sending an email message to the sender. Then you can mark the incident as closed, requiring no further work. Between these extremes, you can establish a policy that automatically encrypts transmissions of confidential data to a business partner. All of these scenarios can be handled automatically without user intervention.
Smart Response	Although the automated response is an important part of the remediation process, <b>SmartResponse</b> is necessary at times, particularly in the case of more serious incidents. Symantec Data Loss Prevention provides a detailed Incident Snapshot with all of the information necessary to determine the next steps in remediation. You can use <b>SmartResponse</b> to manually update incident severity, status, and custom attributes, add comments to the incident. You can move the incident through the remediation workflow to resolve it.
	See "Configuring response rule actions" on page 893.
	The following standard SmartResponse actions are available:
	■ Add Note
	<ul><li>Log to a Syslog Server</li><li>Send Email Notification</li></ul>
	Send Email Notification     Set Status
	See "Configuring the Server FlexResponse action" on page 912.
Distribution of aggregated incident reports	You can create and automatically distribute aggregated incident reports to data owners for remediation.

The Enforce Server handles all of these steps, except for Smart Response. You can handle incidents in an entirely automated way. You can reserve manual intervention (Smart Response) for only the most serious incidents.

See "Network incident snapshot" on page 956.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

# Remediating incidents

When you remediate an incident, you can perform the following actions:

- Set the incident's status or severity.
- Apply a Smart Response rule to the incident.
- Set the incident's custom attributes.
- Add comments to the incident record.
- Remediate incidents by going to an incident list or incident snapshot and selecting actions to perform on one or more incidents.
- Perform some combination of these actions.

You can import a solution pack during installation. Solution packs prepopulate incident lists and incident snapshots with several remediation options and custom attributes. For complete descriptions of all solution packs (including information about all remediation options and custom attributes they contain), refer to the documentation for each of the solution packs in the solutions packs directory in the documentation.

#### To remediate incidents

1 Access an incident list or incident snapshot.

In incident lists, Symantec Data Loss Prevention displays available remediation options in the Incident Actions drop-down menu. The menu becomes active when you select one or more incidents in the list (with the check box). In incident snapshots, Symantec Data Loss Prevention also displays the available remediation options. You can set a Status or Severity from the drop-down menus.

See "Viewing incidents" on page 1018.

You can also edit the **Attributes** and provide related information.

- 2 Take either of the following actions:
  - When you view an incident list, select the incident(s) to be remediated (check the box). You can select incidents individually or select all incidents on the current screen. Then select the wanted action from the Incidents Actions drop-down menu. For example, select Incident Actions > Set Status > Escalated.

You can perform as many actions as needed.

When you view an incident snapshot, you can set the **Status** and **Severity** from the drop-down menus.

If a Smart Response has been previously set up, you can select a Smart Response rule in the remediation bar.

See "About response rules" on page 875.

For example, if one of the Solution Packs was installed, you can select Dismiss False Positive in the remediation bar. When the Execute **Response Rule** screen appears, click **OK**. This Smart Response rule changes the incident status from New to Dismissed and sets the Dismissal Reason attribute to False Positive.

You can perform as many remediation actions as needed.

# **Executing Smart response rules**

When you execute a response rule that sends an email, you can manually compose the contents of the email notification.

Note: Sending an email notification to the sender applies to SMTP incidents only. Also, the notification addressees that are based on custom attributes (such as "manager email") work correctly only if populated by the attribute lookup plug-in.

#### To compose an email notification response

- 1 Enter optional emails for copies in the CC field.
- 2 Select the language.
- 3 Compose or edit the subject and body of the email.
- Insert variables for the fields in the incident. The supported variables appear as links to the right of the editable fields.

For example, if you want to include the policy and rules violated, you might enter:

A message has violated the following rules in \$POLICY\$: \$RULES\$

5 Click **OK** to send the notification.

See "Adding a new response rule" on page 890.

See "About incident remediation" on page 940.

See "Response action variables" on page 946.

### Incident remediation action commands

In an incident list, use the **Incident Actions** drop-down to select remediation actions.

The following incident actions are available for an incident list:

**Add Note** Add a brief note to the selected incident(s). The

> comment appears on the Incident History tab of the Incident Snapshot page for each selected incident.

**Archive** Select one of the following archive actions to set the

archive state for the selected incidents:

 Archive Incidents—Flags the selected incidents as archived.

 Restore Incidents—Restores the selected incidents to the non-archived state.

Do Not Archive—Prevents the selected incidents from being archived.

Allow Archive—Allows the selected incidents to be

archived

See "About incident archiving" on page 1065.

**Delete Incidents** Delete the selected incident(s) from the Symantec Data

Loss Prevention system.

Proceed cautiously when deleting incidents. All data that is associated with the incident(s) is removed. This

operation cannot be reversed.

**Export Selected: CSV** Export the selected incident(s) to a comma-separated

(.csv) file.

**Export Selected: XML** Export the selected incident(s) to an XML file.

**Lookup Attributes** Use the configured lookup plug-ins to look up the

configured attributes.

**Set Attributes** Display the Set Attributes page so you can enter or

edit the attribute values for the selected incident(s).

**Set Data Owner** Set the following Data Owner attributes:

Name

**Email Address** 

**Set Severity** Change the severity that is set for the selected

incident(s) to one of the options under Set Severity.

**Set Status** Change the status of the selected incident(s) to one of

> the options under **Set Status**. A system administrator can customize the options that appear on this list on the

Incident Attributes page.

See "About incident status attributes" on page 1069.

**Run Smart Response** Perform one of the listed responses on the selected

incident(s). When you click a response rule, the Execute

Response Rule page appears.

These manual response rules are available only if you

have permission to remediate.

See "About incident remediation" on page 940.

# Response action variables

Response action variables can be used in response rules.

See "Executing Smart response rules" on page 944.

The response action variables are different for Network Monitor and Network Prevent incidents than for Network Discover and Network Protect incidents.

See "Monitor and Prevent incident variables" on page 946.

See "Mobile incident variables" on page 947.

See "Discover incident variables" on page 948.

## Monitor and Prevent incident variables

The following Network Monitor and Network Prevent variables are available:

**\$BLOCKED\$** Indication of whether or not Symantec Data Loss

Prevention blocked the message (yes or no).

**\$DATAOWNER NAME\$** The person responsible for remediating the

incident. This field must be set manually, or with

one of the lookup plug-ins.

Reports can automatically be sent to the data

owner for remediation.

**\$DATAOWNER EMAIL\$** The email address of the person responsible for

> remediating the incident. This field must be set manually, or with one of the lookup plug-ins.

The ID of the incident. \$INCIDENT\_ID\$

**\$INCIDENT SNAPSHOT\$** The fully qualified URL to the incident snapshot

page for the incident.

**\$MATCH COUNT\$** The incident match count

**\$POLICY NAME\$** The name of the policy that was violated.

\$POLICY\_RULES\$ A comma-separated list of one or more policy rules

that were violated.

**\$RECIPIENTS\$** A comma-separated list of one or more message

recipients.

\$SENDER\$ The message sender.

The severity that is assigned to incident. **\$SEVERITY\$** 

**\$SUBJECT\$** The subject of the message.

# Mobile incident variables

The following Mobile Prevent for Web variables are available:

**\$BLOCKED\$** Indication of whether or not Symantec Data Loss Prevention blocked the

message (yes or no).

**\$DATAOWNER NAME\$** The person responsible for remediating the incident. This field must be set

manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

**\$DATAOWNER EMAIL\$** The email address of the person responsible for remediating the incident. This

field must be set manually, or with one of the lookup plug-ins.

**\$DEVICE INSTANCE ID\$** The specific ID of the mobile device that generated the violation.

**\$ENDPOINT MACHINE\$** The name of the endpoint machine that generated the violation.

\$FILE\_FULL\_PATH\$ The full path to the file in which the incident was found.

\$FILE NAME\$ The name of the file in which the incident was found.

\$FILE PARENT DIRECTORY PATH\$ The path to the parent directory of the file in which the incident was found.

\$INCIDENT\_SNAPSHOT\$ The ID of the incident.

**\$INCIDENT SNAPSHOT\$** The fully qualified URL to the incident snapshot page for the incident. \$MATCH\_COUNT\$ The incident match count.

**\$POLICY NAME\$** The name of the policy that was violated.

**\$POLICY RULES\$** A comma-separated list of one or more policy rules that were violated.

\$PROTOCOL\$ The protocol, device type, or target type that generated the violation.

**\$QUARANTINE PARENT DIRECTORY PATH\$** The path to the parent directory in which the file was quarantined.

**\$RECIPIENTS\$** A comma-separated list of one or more message recipients.

\$SCAN\_DATE\$ The date of the scan that found the incident.

\$SENDER\$ The message sender.

**\$SEVERITY\$** The severity that is assigned to incident.

\$SUBJECT\$ The subject of the message.

**\$TARGET\$** The name of the target in which the incident was found.

## Discover incident variables

The following Network Discover and Network Protect incident variables are available:

**\$DATAOWNER\_NAME\$** The person responsible for remediating the incident. This field must be set

manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

**\$DATAOWNER\_EMAIL\$** The email address of the person responsible for remediating the incident.

This field must be set manually, or with one of the lookup plug-ins.

**\$FILE NAME\$** The name of the file in which the incident was found.

\$INCIDENT ID\$ The ID of the incident

\$MATCH\_COUNT\$ The incident match count.

\$FILE\_PARENT\_DIRECTORY\_PATH\$ The path to the parent directory of the file in which the incident was found.

\$FILE FULL PATH\$ The full path to the file in which the incident was found.

**\$POLICY NAME\$** The name of the policy that was violated.

**\$POLICY RULES\$** A comma-separated list of one or more policy rules that were violated.

**\$QUARANTINE PARENT DIRECTORY PATH\$** The path to the parent directory in which the file was quarantined.

\$SCAN\_DATE\$ The date of the scan that found the incident.

\$SEVERITY\$ The severity that is assigned to incident.

**\$TARGET\$** The name of the target in which the incident was found.

# Remediating Network incidents

This chapter includes the following topics:

- Network incident list
- Network incident list—Actions
- Network incident list—Columns
- Network incident snapshot
- Network incident snapshot—Heading and navigation
- Network incident snapshot—General information
- Network incident snapshot—Matches
- Network incident snapshot—Attributes
- Network summary report

## Network incident list

A network incident list shows multiple network incident records with information about the incident such as: the severity, associated policy, number of matches, and status of the incident. Click a row of the incident list to view more details about a specific incident. Select specific incidents (or groups of incidents) to modify or remediate by clicking the check boxes at the left.

When IPv6 addresses appear in reports, they follow these rules:

Addresses are normalized in the Source IP and Destination IP fields.

- In the **Recipient** (URL) fields, addresses are represented as they have been provided, which is usually a hostname and varies by protocol.
- In the **Sender** fields, representation of addresses varies by protocol.
- Normalized fields are used for IP-based filtering.

When IPv6 addresses appear in incident list filters, they follow these rules:

- Addresses are normalized in the **Source IP** and **Destination IP** fields.
- In the Recipient (URL) field, addresses are represented as they have been provided in the Recipient (URL), Domain, and Sender fields.
- Normalized fields are used for IP-based filtering.

When IPv6 addresses appear in incident details, they follow these rules:

- Addresses are normalized in the **Source IP** and **Destination IP** fields.
- In the Recipient (URL) field, addresses are represented as they have been provided.
- In the **Sender** field, addresses are represented as they have been provided.
- Links to filtered lists behave like user input.

You can view normalized IPv6 addresses in an incident summary:

- Addresses are summarized by the Source IP, Destination IP, Sender, and Domain fields.
- Normalization occurs for fields as it does in the incident details.

You can view non-normalized IPv6 addresses in an incident summary:

- Addresses are summarized by the Source IP, Destination IP, Sender, and Domain fields.
- Normalization occurs for fields as it does in the incident details.

Note: Use caution when you click Select All. This action selects all incidents in the report (not only those on the current page). Any incident command you subsequently apply affects all incidents. To select only the incidents on the current page, select the checkbox at top left of the incident list.

Incident information is divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention sorts incidents by date.

The **Type** column shows the icons that indicate the type of network incident. Table 41-1 describes the icons.

**Table 41-1** Type of network incident

Icon	Description
<u></u>	SMTP
0	The addition of the second icon indicates a message attachment.
8	НТТР
0	Symantec Data Loss Prevention also detects the Yahoo and MSN IM traffic that is tunneled through HTTP.
	The addition of the second icon indicates an attachment to Web-based email.
E.	HTTPS
<u></u>	FTP
	NNTP
8	IM:MSN
•	IM:AIM
**	IM:Yahoo
	TCP:custom_protocol

This column also indicates whether the communication was blocked or altered. Table 41-2 shows the possible values.

Incident block or altered status Table 41-2

Icon	Description
No icon.	Blank if the communication was <b>not</b> blocked.

Table 41-2 Incident block or altered status (continued)

Icon	Description
	Indicates Symantec Data Loss Prevention blocked the communication containing the matched text.
♣	Indicates Symantec Data Loss Prevention removed confidential data from Web postings or Web-based email messages. This icon can also indicate that a file was uploaded to a Web site or attached to a Web-based email message.
+/	Indicates that Symantec Data Loss Prevention added or modified the headers on the message that generated the incident.

Use the following links to learn more about the Network incident list page:

To learn more about	See this section
Columns of the incident list table	See "Network incident list—Columns" on page 955.
Actions to perform on selected incidents	See "Network incident list—Actions" on page 953.
Details of a specific incident	See "Network incident snapshot" on page 956.
Viewing a summary of all network incidents	See "Network summary report" on page 961.
Common features of all Symantec Data Loss	See "About incident reports" on page 1009.
Prevention reports	See "Common incident report features" on page 1039.
	See "Saving custom incident reports" on page 1022.

# Network incident list—Actions

You can select one or more incidents and then remediate them using commands in the Incident Actions drop-down list. The incident commands are as follows:

Reports can automatically be sent to the data

owner for remediation.

Select to set severity.

**Set Severity** 

Action Description Add Note Select to open a dialog box, type a comment, and then click OK. **Archive** Select one of the following archive actions to set the archive state for the selected incidents: Archive Incidents—Flags the selected incidents as archived. ■ Restore Incidents—Restores the selected incidents to the non-archived state. ■ Do Not Archive—Prevents the selected incidents from being archived. ■ Allow Archive—Allows the selected incidents to be archived. See "About incident archiving" on page 1065. **Delete Incidents** Select to delete specified incidents. **Export Selected: CSV** Select to save specified incidents in a comma-separated text (.csv) file or XML file, **Export Selected: XML** which can be displayed in several common applications, such as Microsoft Excel. **Lookup Attributes** Use lookup plug-ins to look up incident custom attributes **Run Smart Response** Select to run a Smart Response rule that you or your administrator configured. (To configure a Smart Response rule, navigate to Policy > Response Rules, click Add Response Rule, and select Smart Response. Set Attributes Select to set attributes for the selected incidents. Set Data Owner Set the data owner name or email address. The data owner is the person responsible for remediating the incident.

Action Description Set Status Select to set status.

See "About incident remediation" on page 940.

See "Network incident list" on page 950.

## Network incident list—Columns

Incident information is divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention lists incidents by date.

The report includes the following columns:

Check boxes that let you select incidents to remediate.

You can select one or more incidents to which to apply commands from the Incident drop-down menu at the top of the list. Click the checkbox at the top of the column to select all incidents on the current page. (Note that you can also click Select All at far right to select all incidents in the report.)

#### Type

The protocol over which the match was detected.

See "Network incident list" on page 950.

#### Subject/Sender/Recipient(s)

Message subject, sender email address or IP address, recipient email address(es), or URL(s).

#### Sent

Date and time the message was sent.

#### ID/Policy

Symantec Data Loss Prevention incident ID number and the policy against which the incident was logged.

#### Matches

Number of matches in the incident.

#### Sev

Incident severity as determined by the severity setting of the rule the incident matched.

The possible values are as follows:

Icon	Description
III	High
III	Medium
III	Low
III	For information only

#### Status

Current incident status.

The possible values are as follows:

- New
- In Process
- **Escalated**
- **False Positive**
- **Configuration Errors**
- Resolved

You or your administrator can add new status designations on the Attribute Setup page.

See "Network incident list" on page 950.

# Network incident snapshot

An incident snapshot provides detailed information about a particular incident. It displays general incident information, matches detected in the intercepted text, and incident attributes. The snapshot also enables you to execute any Smart Response rules that you have configured.

The incident snapshot is divided into three panes, with navigation and Smart Response options. Click on a link to view more help about the incident snapshot:

To learn more about	See the section
Navigation and Smart Response options	See "Network incident snapshot—Heading and navigation" on page 957.
General incident information (left-hand pane)	See "Network incident snapshot—General information" on page 957.

To learn more about	See the section
Matches in incident (middle pane)	See "Network incident snapshot—Matches" on page 960.
Attributes (right-hand pane)	See "Network incident snapshot—Attributes" on page 961.

# Network incident snapshot—Heading and navigation

The following page navigation tools appear near the top of the incident snapshot:

Previous	Displays the previous incident in the source report.
Next	Displays the next incident in the source report.
K.	Returns to the source report (where you clicked the link to get to this screen).
<b>2</b>	Updates the snapshot with any new data, such as a new comment in the History section or a modified status.

If you configured any Smart Response rules, Symantec Data Loss Prevention displays the response options for executing the rules at the top of the page. Depending on the number of Smart Response rules, a drop-down menu may also appear.

See "Network incident snapshot" on page 956.

# Network incident snapshot—General information

The left section of the snapshot displays general incident information. You can click on many values to view an incident list that is filtered on that value. An icon may appear next to the Status drop-down list to indicate whether the request that generated the incident was blocked or altered.

See Table 41-2 on page 952.

The current status and severity of the incident appear to the right of the snapshot heading. To change one of the current values, click on it and choose another value from the drop-down list.

The remaining portion of the general information pane is divided into four tabs.

- Key Info
- History
- Notes
- Correlations

Information in this section is divided into the following categories (not all of which appear for every incident type):

**Table 41-3** Incident general information tabs

able 41-3 Incident general information tabs	
Tab Name	Description
Key Info	The Key Info tab shows the policy that was violated in the incident. It also shows the total number of matches for the policy, as well as matches per policy rule. Click the policy name to view a list of all incidents that violated the policy. Click <b>view policy</b> to view a read-only version of the policy.
	This section also lists other policies that the same file violated. To view the snapshot of an incident that is associated with a particular policy, click <b>go to incident</b> next to the policy name. To view a list of all incidents that the file created, click <b>show all</b> .
	The Key Info tab also includes the following information:
	The name of the detection server that recorded the incident.
	■ The date and time the message was sent
	The sender email or IP address
	The recipient email or IP address(es)
	<ul> <li>The SMTP heading or the NNTP subject heading</li> <li>The Is Archived field displays the archived state of the incident, whether or not the incident is archivable, and allows you to toggle the Do Not Archive flag for the incident.</li> </ul>
	Attachment file name(s). Click to open or save the file. If a response rule tells Symantec Data Loss Prevention to discard the original message, you cannot view the attachment.
	The person responsible for remediating the incident (Data Owner Name). This field must be set manually, or with a lookup plug-in. Reports can automatically be sent to the data owner for remediation.
	If you click on a hyperlinked <b>Data Owner Name</b> , a filtered list of incidents by Data Owner Name is displayed.
	<ul> <li>The email address of the person responsible for remediating the incident (Data Owner Email Address).</li> <li>This field must be set manually, or with a lookup plug-in.</li> <li>If you click on the hyperlinked Data Owner Email</li> <li>Address, a filtered list of incidents by Data Owner Email</li> <li>Address is displayed.</li> </ul>

Table 41-3 Including general information tabs (continued)	
Tab Name	Description
History	View the actions that were performed on the incident. For each action, Symantec Data Loss Prevention displays the action date and time, the actor (a user or server), and the action or the comment.  See "Executing Smart response rules" on page 944.
	See "Manage response rules" on page 889.
Notes	View any notes that you or others have added to the incident. Click <b>Add Note</b> to add a note.
Correlations	You can view a list of those incidents that share attributes of the current incident. For example, you can view a list of all incidents that a single account generated. The <b>Correlations</b> tab shows a list of correlations that match single attributes. Click on attribute values to view lists of those incidents that are related to those values.
	To search for other incidents with the same attributes, click <b>Find Similar</b> . In the <b>Find Similar Incidents</b> dialog box that appears, select the desired search attributes. Then click <b>Find Incidents</b> .
	<b>Note:</b> The list of correlated incidents does not display related incidents that have been archived.

**Table 41-3** Incident general information tabs (continued)

See "Network incident snapshot" on page 956.

See "About incident archiving" on page 1065.

# Network incident snapshot—Matches

Beneath the general information, Symantec Data Loss Prevention displays the message content (if applicable) and the matches that caused the incident. Symantec Data Loss Prevention displays the following types of message content, depending on protocol type:

Protocol	Message content
SMTP	Message body
HTTP	Name value pairs of the HTTP request
FTP	Nothing shown

Protocol	Message content
NNTP	Message body
IM (all providers)	IM conversation
TCP	Data that was transmitted through custom protocol

Matches are highlighted in yellow and organized according to the message component (such as header, body, or attachment) in which they were detected. Symantec Data Loss Prevention displays the total relevant matches for each message component. It shows matches by the order in which they appear in the original text. To view the rule that triggered a match, click on the highlighted match.

See "About the Similarity Threshold and Similarity Score" on page 512.

See "Network incident snapshot" on page 956.

# Network incident snapshot—Attributes

Note: This section appears only if a system administrator has configured custom attributes.

You can view a list of custom attributes and their values, if any have been specified. Click on attribute values to view an incident list that is filtered on that value. To add new values or edit existing ones, click Edit. In the Edit Attributes dialog box that appears, type the new values and click Save.

See "Setting the values of custom attributes manually" on page 1080.

See "Network incident snapshot" on page 956.

# Network summary report

The Network summary report provides summary information about the incidents that are found on your network. You can organize the report by one or two summary criteria. A single-summary report is organized by a single summary criterion, such as the policy that is associated with each incident. A double-summary report is organized by two criteria, such as policy and incident status.

To view the primary criteria and the secondary summary criteria available for the current report, click the Advanced Filters & Summarization bar. The bar is near the top of the report. The Summarize By: listboxes show the primary criteria and the secondary summary criteria. In each listbox, Symantec Data Loss Prevention

displays all out-of-the-box criteria in alphabetical order, followed by any custom criteria that your system administrator has defined. Summary reports take their name from the primary summary criterion (the value of the first listbox). If you rerun a report with new criteria, the report name changes accordingly.

Summary entries are divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time.

Summary report columns Table 41-4

Column name	Description
summary_criterion	This column is named for the primary summary criterion. It lists primary and (for double summaries) secondary summary items. In a Policy Summary, this column is named Policy and it lists policies. Click on a summary item to view a list of incidents that are associated with that item.
Total	The total number of incidents that are associated with the summary item. In a Policy Summary, this column gives the total number of incidents that are associated with each policy.
High	Number of high-severity incidents that are associated with the summary item. (The severity setting of the rule that was matched determines the incident severity.)
Med	Number of medium-severity incidents that are associated with the summary item.
Low	Number of low-severity incidents that are associated with the summary item.
Info	The number of informational incidents that are associated with the summary item.
Bar Chart	A visual representation of the number of incidents (of all severities) associated with the summary item. The bar is broken into proportional, colored sections to represent the various severities.
Matches	Total number of matches associated with the summary item.

If any of the severity columns contain totals, you can click on them to view a list of incidents of the chosen severity.

See "Common incident report features" on page 1039.

See "About dashboard reports and executive summaries" on page 1011.

See "About incident reports" on page 1009.

See "Saving custom incident reports" on page 1022.

# Chapter

# Remediating Endpoint incidents

This chapter includes the following topics:

- Endpoint incident lists
- Endpoint incident snapshot
- Reporting on Endpoint Prevent response rules
- Endpoint incident destination or protocol-specific information
- Endpoint incident summary reports

# **Endpoint incident lists**

An endpoint incident list shows endpoint incidents that contain basic information such as protocol or destination, severity, associated policy, number of matches, and status. Click on any incident to view a snapshot containing more incident details. You can select specific incidents (or groups of incidents) to modify or remediate.

**Note:** Endpoint reports show only the incidents that were captured by Endpoint Prevent. Incidents that were captured by Endpoint Discover appear in Network Discover reports.

Incident information is divided into several columns. Click any column header to sort alpha-numerically by the data in that column. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention lists incidents by date.

The report includes the following columns:

#### ■ Check boxes that let you select incidents to remediate

You can select one or more incidents to which to apply commands from the Incident drop-down menu at the top of the list. Click the checkbox at the top of the column to select all incidents on the current page. (You can click Select All at far right to select all incidents in the report.)

**Table 42-1** Type of endpoint incident

Graphic	Type of incident
<b>o</b>	CD/DVD burner (for example, Windows Media burner)
<b>©</b>	Removable media (for example, a USB flash drive or SD card)
8	Fixed drive (for example, the C:\ drive)
4	Endpoint copy to network share
<u></u>	Email/SMTP
<b>S</b>	НТТР
<b>&amp;</b>	HTTPS
<u></u>	FTP
•	IM:AIM
8	IM: MSN
♥	IM: Yahoo
<b>=</b>	Print/Fax
<b>a</b>	Clipboard
	Application File Access

A response column that indicates whether Symantec Data Loss Prevention blocked an attempted violation or notified the end user about the violation of confidential data.

The possible values are as follows:

- Blank if Symantec Data Loss Prevention did not block the violation or notify the end user
- A red icon indicates the violation was blocked by Symantec Data Loss Prevention, by the user, or if the user cancel option time limit expired.
- A notification icon indicates Symantec Data Loss Prevention notified the end user about the violated confidential data policies. The notification icon also appears if the user allowed the violating data transfer. The icon also appears if the user cancel time limit option has expired and the default action is set to allow data transfers.

The other columns of this section appear as follows:

Table 42-2 Endpoint incident columns

Column	Definition
File Name/Machine/User/Subject/Recipient	File name, computer, endpoint user (domain and logon name), subject title (if Email/SMTP violation), and recipient user that is associated with the incident
Occurred On Date	<ul> <li>Incident date and time</li> <li>Reported On Date</li> <li>Time and date that the incident was reported. If the endpoint is disconnected from the corporate network, incidents are reported when the connection is restored.</li> </ul>
ID/Policy	Symantec Data Loss Prevention incident ID number and the policy against which the incident was logged
Matches	Number of matches in the incident

able 12 2 Endpoint motable columns (continued)	
Column	Definition
Severity	Incident severity as determined by the severity setting of the rule the incident matched.
	The possible values are as follows:
	<ul><li>High</li><li>Medium</li><li>Low</li><li>For information only</li></ul>
Status	Current incident status The possible values are as follows:  New In Process Escalated False positive Configuration Errors Resolved

Endpoint incident columns (continued) **Table 42-2** 

You or your administrator can add new status designations on the Attribute Setup page.

See "Endpoint incident snapshot" on page 967.

See "About incident remediation" on page 940.

See "About incident reports" on page 1009.

See "Saving custom incident reports" on page 1022.

# **Endpoint incident snapshot**

An incident snapshot provides detailed information about a particular Endpoint Prevent incident. It displays general incident information, matches detected in the intercepted text, and details about attributes, incident history, and the violated policy. You can also search for similar incidents in the Correlations area.

Note: Endpoint Discover incidents are captured in Network Discover reports.

See "Discover incident lists" on page 995.

Current status and severity appear under the snapshot heading. To change one of the current values, click on it and choose another value from the drop-down list. If any action icon is associated, it also appears here.

If you have configured any Smart Response rules, Symantec Data Loss Prevention displays a Remediation bar (under the Status bar). The Remediation bar includes options for executing the rules. Depending on the number of Smart Response rules, a drop-down menu may also appear.

The top left section of the snapshot displays general incident information. You can click most information values to view an incident list that is filtered on that value. Information in this section is divided into the following categories (not all of which appear for every incident type):

Table 42-3 Type of incident

Icon	Incident type
<b>o</b>	CD/DVD burners (for example, Windows Media burner)
<b>©</b>	Removable media (for example, a USB flash drive or SD card)
8	Local drive
	Network Share
<u></u>	Email/SMTP
8	НТТР
<b>&amp;</b>	HTTPS/SSL
<u> </u>	FTP
•	IM:AIM
8	IM: MSN
ಳ	IM: Yahoo
<b>=</b>	Print/Fax

Type of incident (continued) Table 42-3

Icon	Incident type
	Clipboard
	Application File Access

The following table contains the other informational sections:

**Table 42-4** Incident sections

Section	Description
Server	Name of the Endpoint Server that detected the incident for two-tier detection. Or, it is the name of the Endpoint Server that received the incident from the Symantec DLP Agent.
Agent response	The Endpoint Block, Endpoint Notify, Endpoint Quarantine, Endpoint FlexResponse, or User Cancel action, if any. The possible values are as follows:
	Blank or no icon if Symantec Data Loss     Prevention did not block the copy or notify the end user.
	<ul> <li>A red circle icon indicates Symantec Data Loss Prevention blocked confidential data.</li> <li>A message icon indicates Symantec Data Loss Prevention notified the end user that the data is confidential.</li> </ul>
	See Reporting on Endpoint Prevent Response Rules.
Incident Occurred On	Date and time the incident occurred.
Incident Reported On	Date and time the Endpoint Server detected the incident.
Is Archived	Displays the archived state of the incident, whether or not the incident is archivable, and allows you to toggle the <b>Do Not Archive</b> flag for the incident. See "About incident archiving" on page 1065.

Incident sections (continued) **Table 42-4** 

Section	Description
User	Endpoint user name (for example, MYDOMAIN\bsmith).
User Justification	The justification label precedes by the text that is presented to the end user in the on-screen notification (for example, Manager Approved: "My manager approved the transfer of this data.") Symantec Data Loss Prevention uses the label for classification and filtering purposes in reports, but the endpoint user never sees it. Click the label to view a list of incidents in which the end user chose this justification.
Machine Name	Computer on which the incident occurred.
Machine IP (Corporate)	The IP address of the violating computer if the computer was on the corporate network.
File name	Name of the file that violated the policy. The file name field appears only for fixed-drive incidents.
Quarantine Result	If you have Endpoint Discover: Quarantine response rules configured, you may see one of the following quarantine scenarios:  File Quarantined Quarantine Failed Quarantine Result Timeout
Quarantine Location	Displays the file path of the secure location where the file was moved.
Quarantine Details	Displays the reason that the quarantine task failed to move the confidential file. For example, the action may fail because the source file is missing, or the credentials to access the secure location are incorrect.  The Quarantine Details file also displays information if the status of the quarantined file is unknown because of a Quarantine Result Timeout event.

Incident sections (continued) **Table 42-4** 

Section	Description
Endpoint Location	Indicates whether or not the endpoint was connected to the corporate network at the time the incident occurred.
Application Name	The name of the application that caused the incident.
Destination	The destination location or file path for the confidential data, depending on the device or protocol.
Destination IP	The destination IP address for the confidential data. The Destination IP address appears only for specific network incidents.
Source	The original file or data for the violation. The source primarily appears in file-transfer incidents.
Sender	The sender of the confidential data for network violations.
Recipient	The intended recipient of the confidential data for network violations.
FTP User Name	The originating user name for violating FTP transfers.
Attachments	The associated file(s) or attachments sent (for network incidents). If your administrator has configured Symantec Data Loss Prevention to retain endpoint incident data, you can click on a file name to view file contents.
Data Owner	The specified owner of the confidential data.
Data Owner Email Address	The email address for the owner of the confidential data.
Access information	The available ACL information. Only applicable to Endpoint Discover and Endpoint Prevent local drive monitoring.
	See "Incident snapshot access information section" on page 1044.

Other sections of the incident snapshot are common across all Symantec Data Loss Prevention products. These common sections include:

- Incident snapshot matches See "Incident snapshot matches section" on page 1044.
- Incident snapshot policy section See "Incident snapshot policy section" on page 1043.
- Incident snapshot correlations section See "Incident snapshot correlations tab" on page 1043.
- Incident snapshot attributes section. (This section appears only if a system administrator has configured custom attributes.) See "Incident snapshot policy section" on page 1043.
- Incident snapshot history section See "Incident snapshot history tab" on page 1042.

The Endpoint incident snapshot also contains two sections that are not common across other product lines. Those sections are:

- Destination or protocol-specific information See "Endpoint incident destination or protocol-specific information" on page 974.
- Reporting on Endpoint Prevent response rules See "Reporting on Endpoint Prevent response rules" on page 972.

# Reporting on Endpoint Prevent response rules

If user activity on the endpoint triggers more than one response rule, Symantec Data Loss Prevention determines which policy to apply based on an established order of precedence. Only the response rule that is associated with the prevailing policy is executed. Symantec Data Loss Prevention creates incidents for all policies that are violated. It indicates (in the relevant incident snapshots) that the response rules were superseded.

See "Endpoint incident snapshot" on page 967.

By default, the following list is the main order of precedence for Endpoint Prevent incidents:

- Block
- User Cancel
- Endpoint FlexResponse
- Notify

Note: For Endpoint Discover, Quarantine incidents always take precedence over Endpoint FlexResponse incidents.

Be aware of the following behavior regarding reporting of superseded incidents:

- The snapshot of a superseded Endpoint Block or User Cancel incident still displays the **Blocked** icon, because Symantec Data Loss Prevention did block the content in question. The icon also indicates if the content was blocked because the user elected to block the content. Alternately, the icon indicates that the user cancel time limit was exceeded and the content was blocked.
- The snapshot of a superseded Endpoint Notify incident does **not** include the **Notify** icon. The Notify icon is not included because Symantec Data Loss Prevention did not display the particular on-screen notification that was configured in the policy.
- The snapshot of a superseded Endpoint Quarantine incident displays the **Blocked** icon because the data did not move out of the secured area. The icon also indicates if the content was blocked because the user elected to block the content. Alternately, the icon indicates that the user cancel time limit was exceeded and the content was blocked. The History tab of the incident snapshot always displays information on whether the Endpoint FlexResponse rule was successful.
- The snapshot of a superseded Endpoint FlexResponse incident displays the **Blocked** icon because the data did not move out of the secured area. The icon also indicates if an Endpoint Quarantine response rule was activated.

If you have configured Endpoint Prevent response rules to display on-screen notifications prompting users to justify their actions, the following statements are true:

- Symantec Data Loss Prevention displays the user justification in the snapshots of all the incidents that are generated by the policies that include the executed response rule.
- Symantec Data Loss Prevention displays the justification Superseded Yes in the snapshots of all superseded incidents that do not include the executed response rule.
- If there is no user to enter a justification, for example if a user accesses a remote computer, the justification reads N/A.

See "Network incident snapshot" on page 956.

See "Configuring response rule conditions" on page 892.

See "About incident reports" on page 1009.

See "Manage response rules" on page 889.

# **Endpoint incident destination or protocol-specific** information

Depending on the type of incident, additional information that is associated with the incident snapshot is visible.

Destination or protocol-specific information Table 42-5

Destination or protocol	Description
URL	For network incidents, denotes the URL where the incident occurred.
Source IP and Port	For network incidents, denotes the IP address or port of the endpoint that originated the incident. This information is only shown if the incident is created on this endpoint.
Destination IP and Port	The IP address of the destination endpoint that is associated with the incident. This information is only shown if the incident is created on this endpoint.
Sender/Recipient Email	For Email/SMTP and IM incidents, incidents also contain the email addresses of the sender and recipient. The sender or recipient email address are only shown if the incident occurs on them.
Subject	The subject line of the Email/SMTP message is displayed.
FTP user name at the FTP Destination	For FTP incidents, the user name at the FTP destination is displayed.
Server IP	For FTP incidents, the server IP address is shown.
File Name/Location	For print/fax incidents, the name of the file and the location of the file on the endpoint is displayed.
Print Job Name	For print/fax incidents, the print job name is the file name of the printing job that generated the incident.

Destination or protocol	Description
Printer Name/Type	For print/fax incidents, the printer name and type are only displayed if the file cannot be named through from the Print Job name. Or, if the file was generated from an Internet browser.
Application Window	For clipboard incidents, the application window is the application name from which the contents of the clipboard were taken.
Title Bar	For clipboard incidents, the title bar is the window from which the data was copied.

**Table 42-5** Destination or protocol-specific information (continued)

See "Endpoint incident snapshot" on page 967.

## **Endpoint incident summary reports**

Endpoint incident summary reports provide information about those Endpoint incidents that has been summarized by specific criteria. You can summarize incidents by one or more types of criteria. A single-summary report is organized by a single summary criterion, such as the policy that is associated with each incident. A double-summary report is organized by two or more criteria, such as policy and incident status.

**Note:** Endpoint reports show only the incidents that are captured by Endpoint Prevent. Incidents from Endpoint Discover appear in Network Discover reports.

To view the primary and the secondary summary criteria available for the report, go to the Summarize By link. Click Edit. In the Primary and Secondary drop-down menus, Symantec Data Loss Prevention displays all of the criteria in alphabetical order, followed by custom criteria your system administrator defined. You can select criteria from the Primary and Secondary drop-down menus and then click Run Now to create a new summary report. Summary reports take their name from the primary summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

See "About filters and summary options for reports" on page 1046.

Summary entries are divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time.

Endpoint incident summary report details **Table 42-6** 

Field	Description
Summary criteria	This column contains the name of whichever summery criteria you selected. If you select a primary and a secondary summary criteria, only the primary criteria is displayed.
Total	Total number of the incidents that are associated with the summary item. For example, in a Policy Summary this column gives the total number of incidents that are associated with each policy.
High	Number of high-severity incidents that are associated with the summary item. (The severity setting of the rule that was matched determines the level of severity.)
Med	Number of medium-severity incidents that are associated with the summary item.
Low	Number of low-severity incidents that are associated with the summary item.
Info	Number of the informational incidents that are associated with the summary item.
Bar Chart	A visual representation of the number of incidents (of all severities) associated with the summary item. The bar is broken into proportional colored sections that represent the various severities.
Matches	Total number of matches associated with the summary item.
	If any of the severity columns contain totals, you can click on them to view a list of incidents of the chosen severity.

# Remediating Mobile incidents

This chapter includes the following topics:

- Mobile incident reports
- Mobile incident snapshot
- Mobile incident list
- Mobile Prevent incident list—Actions
- Mobile incident list—Columns
- Mobile incident snapshot—Heading and navigation
- Mobile incident snapshot—General information
- Mobile incident snapshot—Matches
- Mobile incident snapshot—Attributes
- Mobile summary report

## Mobile incident reports

Use Mobile incident reports to monitor and respond to Mobile incidents. You can save, send, export, or schedule Symantec Data Loss Prevention reports.

In the Enforce Server administration console, on the **Incidents** menu, click **Mobile**. This incident report displays all incidents for any target that is a mobile device. You can select the standard reports for all incidents, new incidents, policy summary, status by policy, or high-risk senders.

Summaries and filter options can select which incidents to display.

See "About filters and summary options for reports" on page 1046.

You can create custom reports with combinations of filters and summaries to identify the incidents to remediate.

See "About custom reports and dashboards" on page 1019.

See "Mobile incident list" on page 978.

## Mobile incident snapshot

An incident snapshot provides detailed information about a particular incident. It displays general incident information, matches detected in the intercepted text, and incident attributes. The snapshot also enables you to execute any Smart Response rules that you have configured.

The incident snapshot is divided into three panes, with navigation and Smart Response options. Click on a link to view more help about the incident snapshot:

To learn more about	See the section
Navigation and Smart Response options	See "Mobile incident snapshot—Heading and navigation" on page 983.
General incident information (left-hand pane)	See "Mobile incident snapshot—General information" on page 983.
Matches in incident (middle pane)	See "Mobile incident snapshot—Matches" on page 985.
Attributes (right-hand pane)	See "Mobile incident snapshot—Attributes" on page 986.

### Mobile incident list

A Mobile incident list shows multiple mobile incident records with information about the incident such as: the severity, associated policy, number of matches, and status of the incident. Click a row of the incident list to view more details about a specific incident. Select specific incidents (or groups of incidents) to modify or remediate by clicking the check boxes at the left.

Note: Use caution when you click Select All. This action selects all incidents in the report (not only those on the current page). Any incident command you subsequently apply affects all incidents. To select only the incidents on the current page, select the checkbox at top left of the incident list.

Incident information is divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention sorts incidents by date.

The **Type** column shows the icons that indicate the type of mobile incident. Table 43-1 describes the icons.

**Table 43-1** Type of Mobile Prevent incident

Icon	Description
3	НТТР
0	Symantec Data Loss Prevention also detects the Yahoo and MSN IM traffic that is tunneled through HTTP.
	The addition of the second icon indicates an attachment to Web-based email.
de la companya de la	HTTPS
<b></b>	FTP

This column also indicates whether the communication was blocked or altered. Table 43-2 shows the possible values.

Mobile Prevent block or altered status **Table 43-2** 

Icon	Description
No icon.	Blank if the communication was <b>not</b> blocked.
•	Indicates Symantec Data Loss Prevention blocked the communication containing the matched text.
*	Indicates Symantec Data Loss Prevention removed confidential data from Web postings or Web-based email messages. This icon can also indicate that a file was uploaded to a Web site or attached to a Web-based email message.
+/	Indicates that Symantec Data Loss Prevention has added or modified the headers on the message that generated the incident.

Use the following links to learn more about the Mobile incident list page:

To learn more about	See this section
Columns of the incident list table	See "Mobile incident list—Columns" on page 981.
Actions to perform on selected incidents	See "Mobile Prevent incident list—Actions" on page 980.
Details of a specific incident	See "Mobile incident snapshot" on page 978.
Viewing a summary of all mobile incidents	See "Mobile summary report" on page 986.
Features that are common to all	See "About incident reports" on page 1009.
Symantec Data Loss Prevention reports	See "Common incident report features" on page 1039.
	See "Saving custom incident reports" on page 1022.

### Mobile Prevent incident list—Actions

You can select one or more incidents and then remediate them using commands in the Incident Actions drop-down list.

Note: No remediation actions are available in Mobile Email Monitor.

The incident commands are as follows:

Action	Description
Add Note	Select to open a dialog box, type a comment, and then click <b>OK</b> .

Action	Description
Archive	Select one of the following archive actions to set the archive state for the selected incidents:
	<ul> <li>Archive Incidents—Flags the selected incidents as archived.</li> <li>Restore Incidents—Restores the selected incidents to the non-archived state.</li> <li>Do Not Archive—Prevents the selected incidents from being archived.</li> <li>Allow Archive—Allows the selected incidents to be archived.</li> </ul>
	See "About incident archiving" on page 1065.
Delete Incidents	Select to delete specified incidents.
Export Selected: CSV	Select to save specified incidents in a
Export Selected: XML	comma-separated text (.csv) file or XML file, which can be displayed in common applications, such as Microsoft Excel.
Lookup Attributes	Use lookup plug-ins to look up incident custom attributes.
Set Attributes	Select to set attributes for the selected incidents.
Set Severity	Select to set severity.
Set Status	Select to set status.

See "About incident remediation" on page 940. See "Mobile incident snapshot" on page 978.

## Mobile incident list—Columns

Incident information is divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention lists incidents by date.

The report includes the following columns:

Checkboxes that let you select incidents to remediate.

You can select one or more incidents to which to apply commands from the Incident drop-down menu at the top of the list. Click the checkbox at the top of the column to select all incidents on the current page. You can also click **Select All** at far right to select all incidents in the report.

Note: No remediation actions are available for Mobile Email Monitor.

#### Type

The protocol over which the match was detected.

#### Subject/Sender/Recipient(s)

Message subject, sender email address or IP address, recipient email address(es), or URL(s).

#### Sent

Date and time the message was sent.

#### ID/Policy

Symantec Data Loss Prevention incident ID number and the policy against which the incident was logged.

#### Matches

Number of matches in the incident.

#### Severity

Incident severity as determined by the severity setting of the rule the incident matched.

The possible values are as follows:

Icon	Description
III	High
III.	Medium
III	Low
III	For information only

#### Status

Current incident status.

The possible values are as follows:

#### New

- In Process
- **Escalated**
- **False Positive**
- Configuration Errors
- Resolved

You or your administrator can add new status designations on the Attribute Setup page.

## Mobile incident snapshot—Heading and navigation

The following page navigation tools appear near the top of the incident snapshot:

Previous	Displays the previous incident in the source report.
Next	Displays the next incident in the source report.
K.	Returns to the source report (where you clicked the link to get to this screen).
<b>2</b>	Updates the snapshot with any new data, such as a new comment in the History section or a modified status.

See "Mobile incident snapshot" on page 978.

## Mobile incident snapshot—General information

The left section of the snapshot displays general incident information. You can click on many values to view an incident list that is filtered on that value. An icon may appear next to the Status drop-down list to indicate whether the request that generated the incident was blocked or altered.

See Table 41-2 on page 952.

The current status and severity of the incident appear to the right of the snapshot heading. To change one of the current values, click on it and choose another value from the drop-down list.

The remaining portion of the general information pane is divided into four tabs.

Key Info

- History
- Notes
- Correlations

Information in this section is divided into the following categories (not all of which appear for every incident type):

Incident general information tabs Table 43-3

Tab Name	Description
Tab Ivallie	Description
Key Info	The Key Info tab shows the policy that was violated in the incident. It also shows the total number of matches for the policy, as well as matches per policy rule. Click the policy name to view a list of all incidents that violated the policy. Click <b>view policy</b> to view a read-only version of the policy.
	This section also lists other policies that the same file violated. To view the snapshot of an incident that is associated with a particular policy, click <b>go to incident</b> next to the policy name. To view a list of all incidents that the file created, click <b>show</b> all.
	The Key Info tab also includes the following information:
	<ul> <li>The name of the detection server that recorded the incident.</li> <li>The date and time the message was sent.</li> <li>The sender email or IP address.</li> <li>The recipient email or IP address(es).</li> <li>The SMTP heading or the NNTP subject heading.</li> <li>Attachment file name(s). Click to open or save the file. If a response rule tells Symantec Data Loss Prevention to discard the original message, you cannot view the attachment.</li> <li>The person responsible for remediating the incident (Data Owner Name). This field must be set manually. Reports can automatically be sent to the data owner for remediation.</li> </ul>
	If you click on a hyperlinked <b>Data Owner Name</b> , a filtered list of incidents by Data Owner Name is displayed.  The email address of the person responsible for remediating the incident ( <b>Data Owner Email Address</b> ). This field must be set manually.  If you click on the hyperlinked <b>Data Owner Email Address</b> , a filtered list of incidents by Data Owner Email Address is displayed.

Tab Name	Description
History	View the actions that were performed on the incident. For each action, Symantec Data Loss Prevention displays the action date and time, the actor (a user or server), and the action or the comment.
	See "Executing Smart response rules" on page 944.
	See "Manage response rules" on page 889.
Notes	View any notes that you or others have added to the incident. Click <b>Add Note</b> to add a note.
Correlations	You can view a list of those incidents that share attributes of the current incident. For example, you can view a list of all incidents that a single account generated. Symantec Data Loss Prevention shows a list of correlations that match single attributes. Click on attribute values to view lists of those incidents that are related to those values.
	To search for other incidents with the same attributes, click <b>Find Similar</b> . In the <b>Find Similar Incidents</b> dialog box that appears, select the desired search attributes. Then click <b>Find Incidents</b> .

Table 43-3 Incident general information tabs (continued)

See "Mobile incident snapshot" on page 978.

## Mobile incident snapshot—Matches

Beneath the general information, Symantec Data Loss Prevention displays the message content (if applicable) and the matches that caused the incident. Symantec Data Loss Prevention displays the following types of message content, depending on protocol type:

Protocol	Message content
HTTP/S	Name value pairs of the HTTP/S request
FTP	Nothing shown

Matches are highlighted in yellow and organized according to the message component (such as header, body, or attachment) in which they were detected. Symantec Data Loss Prevention displays the total relevant matches for each message component. It shows matches by the order in which they appear in the original text. To view the rule that triggered a match, click on the highlighted match. See "About the Similarity Threshold and Similarity Score" on page 512.

See "Mobile incident snapshot" on page 978.

## Mobile incident snapshot—Attributes

Note: This section appears only if a system administrator has configured custom attributes.

You can view a list of custom attributes and their values, if any have been specified. Click on attribute values to view an incident list that is filtered on that value. To add new values or edit existing ones, click Edit. In the Edit Attributes dialog box that appears, type the new values and click Save.

See "Setting the values of custom attributes manually" on page 1080.

See "Mobile incident snapshot" on page 978.

## Mobile summary report

The Mobile summary report provides summary information about the incidents that are generated on your mobile devices. You can organize the report by one or two summary criteria. A single-summary report is organized by a single summary criterion, such as the policy that is associated with each incident. A double-summary report is organized by two criteria, such as policy and incident status.

To view the primary criteria and the secondary summary criteria available for the current report, click the Advanced Filters and Summarization bar. The bar is near the top of the report. The Summarize By: listboxes show the primary criteria and the secondary summary criteria. In each listbox, Symantec Data Loss Prevention displays all detection criteria in alphabetical order, followed by any custom criteria that your system administrator has defined. Summary reports take their name from the primary summary criterion (the value of the first listbox). If you rerun a report with new criteria, the report name changes accordingly.

Summary entries are divided into several columns. Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time.

Table 43-4 Summary report columns

Column name	Description
summary_criterion	This column is named for the primary summary criterion. It lists primary and (for double summaries) secondary summary items. In a Policy Summary, this column is named Policy and it lists policies. Click on a summary item to view a list of incidents that are associated with that item.
Total	The total number of incidents that are associated with the summary item. In a Policy Summary, this column gives the total number of incidents that are associated with each policy.
High	Number of high-severity incidents that are associated with the summary item. (The severity setting of the rule that was matched determines the incident severity.)
Med	Number of medium-severity incidents that are associated with the summary item.
Low	Number of low-severity incidents that are associated with the summary item.
Info	The number of informational incidents that are associated with the summary item.
Bar Chart	A visual representation of the number of incidents (of all severities) associated with the summary item. The bar is broken into proportional, colored sections to represent the various severities.
Matches	Total number of matches associated with the summary item.

If any of the severity columns contain totals, you can click on them to view a list of incidents of the chosen severity.

See "Common incident report features" on page 1039.

See "About dashboard reports and executive summaries" on page 1011.

See "About incident reports" on page 1009.

See "Saving custom incident reports" on page 1022.

# Remediating Discover incidents

This chapter includes the following topics:

- About reports for Network Discover
- About incident reports for Network Discover
- Discover incident reports
- Discover incident snapshots
- Working around the issues with go to links in the Firefox browser
- Discover incident lists
- Network Discover incident actions
- Network Discover incident entries
- Discover summary reports

## **About reports for Network Discover**

Symantec Data Loss Prevention has reports for incidents, Network Discover targets, scan details, and scan history.

The Network Discover incident reports contain details about the confidential data that is exposed.

See "About incident reports for Network Discover" on page 989.

For information about Network Discover targets and scan history, go to **Manage > Discover Scanning > Discover Targets**, then select one of the Discover targets from the list. For information about Network Discover scan details, go to **Manage** 

> Discover Scanning > Scan History, then select one of the Discover scans from the list.

See "Managing Network Discover target scans" on page 1209.

Table 44-1 lists the Network Discover reports.

**Table 44-1 Network Discover Reports** 

Report	Navigation
Network Discover Targets	This report is on the Enforce Server administration console, Manage menu, Discover Scanning > Discover Targets.
	See "About the Network Discover scan target list" on page 1210.
Scan Status	This report is on the Enforce Server administration console, Manage menu, Discover Scanning > Discover Servers.
	See "Viewing Network Discover server status" on page 1219.
Scan History (single target)	This report is from the Enforce Server administration console, Manage menu, Discover Scanning > Discover Targets. Click the link in the Scan Status column to see the history of a particular scan target.
	See "About Network Discover scan histories" on page 1213.
Scan History (all targets)	This report is from the Enforce Server administration console, Manage menu, Discover Scanning > Scan History.
	See "About Network Discover scan histories" on page 1213.
Scan Details	This report is from the Enforce Server administration console, Manage menu, Discover Scanning > Scan History. Click the link in the Scan Status column to see the scan details.
	See "About Network Discover scan details" on page 1215.

## About incident reports for Network Discover

Use incident reports to track and respond to Network Discover incidents. You can save, send, export, or schedule Symantec Data Loss Prevention reports.

See "About Symantec Data Loss Prevention reports" on page 1006.

In the Enforce Server administration console, on the Incidents menu, click Discover This incident report displays all incidents for all Discover targets. You can select the standard reports for all incidents, new incidents, target summary, policy by target, status by target, or top shares at risk.

Summaries and filter options can select which incidents to display.

See "About custom reports and dashboards" on page 1019.

See "About filters and summary options for reports" on page 1046.

You can create custom reports with combinations of filters and summaries to identify the incidents to remediate.

For example you can create the following reports:

- A summary report of the number of incidents in each remediation category. Select the summary **Protect Status**.
- A report of all the incidents that were remediated with copy or quarantine. Select the filter Protect Status with values of File Copied and File Quarantined.
- A report of the Network Discover incidents that have not been seen before (to identify these incidents and notify the data owners to remediate them). Select the filter **Seen Before?**. Set a value of **No**.
- A report of the Network Discover incidents that are still present (to know which incidents to escalate for remediation). Select the filter Seen Before?. Set a value of Yes.
- A report using the summary filters, such as months since first detected. Select the summary Months Since First Detected.

## Discover incident reports

Use Network Discover incident reports to monitor and respond to Network Discover incidents. You can save, send, export, or schedule Symantec Data Loss Prevention reports.

In the Enforce Server administration console, on the Incidents menu, click Discover This incident report displays all incidents for all Discover targets. You can select the standard reports for all incidents, new incidents, target summary, policy by target, status by target, or top shares at risk.

Summaries and filter options can select which incidents to display.

See "Incident report filter and summary options" on page 1040.

You can create custom reports with combinations of filters and summaries to identify the incidents to remediate.

See "About custom reports and dashboards" on page 1019.

Network Discover has the following types of reports:

 Incident list See "Discover incident lists" on page 995.

- Incident summary See "Discover summary reports" on page 999.
- Incident snapshot See "Discover incident snapshots" on page 991.

## Discover incident snapshots

An incident snapshot provides detailed information about a particular incident. It displays general incident information, matches detected in the intercepted text, and details about policy, attributes, and incident history. You can also search for similar incidents in the Correlations area.

Current status and severity appear under the snapshot heading. To change one of the current values, click it and choose another value from the drop-down list.

Use the icons at the top right to print the report, or send it as email. To send reports, you or your administrator must first enable report distribution in system settings.

See "Configuring the Enforce Server to send email alerts" on page 146.

If any Smart Response rules are set up. Symantec Data Loss Prevention displays a remediation bar that includes buttons for executing the rules. Depending on the number of Smart Response rules, a drop-down menu may also appear.

See "About incident remediation" on page 940.

Incident data is divided into the following sections:

#### Key Info tab

#### Policy Matches

See "Incident snapshot policy section" on page 1043.

#### **Incident Details**

The following details are included:

Server	Name of the Discover Server that detected the incident.
Remediation Detection Status	The latest remediation status of the file that generated the incident.
Target	Network Discover target name.
Scan	The date and time of the scan that registered the incident.
Detection Date	The date and time that the incident was detected.
Seen Before	No, if this incident was not previously detected. Yes, if this incident was previously detected.

Subject Email subject for integrated Exchange scans.

Sender Email sender for integrated Exchange scans.

Recipient Email recipient for integrated Exchange scans.

File Location Location of the file, repository, or item.

> Click go to file to view the item or file, or go to directory to view the directory. If you view an Endpoint Discover incident, you do not see the go to file or go to directory links.

In the Firefox browser, these links do not work without

additional setup.

See "Working around the issues with go to links in the Firefox

browser" on page 994.

Is Archived Displays the archived state of the incident, whether or not the

> incident is archivable, and lets you toggle the **Do Not Archive** flag for the incident. See "About incident archiving" on page 1065.

URI For SharePoint, this URL is the item on the SharePoint server.

Click this URL to go to the item on the SharePoint server.

Document Name File or item name(s)

File Owner Creator of the file or item.

> For SharePoint and Exchange incident snapshots the File Owner is listed as unknown because it is not applicable to

these target types.

Extraction Date Date custom target adapter was run (Applies to custom targets

only.)

Scanned Machine Host name of the scanned computer.

For SharePoint this name is the web application name.

Notes Database Name of the Lotus Notes database (Applies to Lotus Notes

only.)

File Created The date and time that the file or item was created

Last Modified Date and time of last change to the file or item.

Last Accessed Date and time of last user access to the file or item.

For SharePoint, this date is not valid.

Data Owner Name

The person responsible for remediating the incident. This field must be set manually, or with a lookup plug-in.

Reports can automatically be sent to the data owner for remediation.

If you click on the hyperlinked Data Owner Name, a filtered list of incidents by Data Owner Name is displayed.

Data Owner Email Address

The email address of the person responsible for remediating the incident. This field must be set manually, or with a lookup plug-in.

If you click on the hyperlinked Data Owner Email Address, a filtered list of incidents by Data Owner Email Address is displayed.

#### Access Information

See "Incident snapshot access information section" on page 1044. For SharePoint incident snapshots, the permission levels show the permissions from SharePoint, for example Contribute or Design. The list in the incident snapshot shows only the first 50 entries. All the ACL entries can be exported to a CSV file. The permissions are comma-separated. Users or groups having Limited Access permission levels are not recorded or shown.

#### Message Body

For a SharePoint list item, the message body shows the name and value pairs in the list.

#### Matches and file content

See "Incident snapshot matches section" on page 1044.

#### Attributes

See "Incident snapshot attributes section" on page 1043.

#### History tab

See "Incident snapshot history tab" on page 1042.

#### Notes tab

The notes tab displays any notes for this incident.

#### Correlations tab

See "Incident snapshot correlations tab" on page 1043.

See "Discover incident reports" on page 990.

## Working around the issues with go to links in the Firefox browser

In the Firefox browser, when you view file system incidents, the go to file and go to directory links next to the File Location field do not work.

To go to the file or directory, take one of the following actions:

Right-click the go to file and go to directory link and select Copy Link Location. Open a new browser window (or tab) and paste the URL into the address bar. Press Enter. You must do this copy and paste each time you want to use these links.

Modify Firefox user preferences on the computer on which you use Firefox (not on the Enforce Server host).

#### To modify Firefox user preferences

Go to the Firefox user preferences directory.

For Windows 7, Vista, this directory is

C:\Users\user name\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default, where user\_name is your user name and xxxxxxxx is a random string of characters.

```
For Windows XP, or 2000, this directory is C:\Documents and
Settings\user name\Application
Data\Mozilla\Firefox\Profiles\xxxxxxx.default, where user name is
your user name and xxxxxxxx is a random string of characters.
```

- Look for the user. is file. If it does not exist, create it using a text editor. If it does exist, open it. (Note that you can create or rename the file with a .txt file extension, to edit it with a text editor.)
- 3 Add the following lines:

```
user pref("capability.policy.policynames", "localfilelinks");
user pref("capability.policy.localfilelinks.sites", "enforce url");
user pref("capability.policy.localfilelinks.checkloaduri.enabled",
     "allAccess");
```

where enforce url is the Enforce Server URL as it appears in your browser address bar, up to but not including the first slash (for example, https://enforce.server.name).

4 Save the file (renaming it with a .js file extension, if you changed it for editing purposes), and restart Firefox.

### Discover incident lists

A Network Discover incident list shows the incidents that are reported during Network Discover scans (including the incidents from Endpoint Discover). Individual incident records contain information such as severity, associated policy, number of matches, and status.

See "Network Discover incident entries" on page 996.

You can click on any incident to view a snapshot containing more details.

You can select specific incidents (or a group of incidents) to modify or remediate.

See "Network Discover incident actions" on page 995.

See "Discover incident reports" on page 990.

### **Network Discover incident actions**

You can select one or more incidents and then remediate them using commands in the Incident Actions drop-down list.

The incident commands are as follows:

#### Add Note

Select to open a dialog box, type a comment, and then click **OK**.

#### Archive

Select one of the following archive actions to set the archive state for the selected incidents:

- Archive Incidents—Flags the selected incidents as archived.
- Restore Incidents—Restores the selected incidents to the non-archived state.
- Do Not Archive—Prevents the selected incidents from being archived.
- Allow Archive—Allows the selected incidents to be archived.

See "About incident archiving" on page 1065.

#### Delete Incidents

Select to delete specified incidents.

#### Set Attributes

Select to set attributes for the selected incidents.

#### Export Selected: CSV

Select to save specified incidents in a comma-separated text (.csv) file, which can be displayed in several common applications, such as Microsoft Excel.

#### Export Selected: XML

Select to save specified incidents in an XML file, which can be displayed in several common applications.

#### Lookup Attributes

Use the lookup plug-ins to look up incident custom attributes.

#### Set Data Owner

Set the data owner name or email address. The data owner is the person responsible for remediating the incident.

Reports can automatically be sent to the data owner for remediation.

#### Set Severity

Select to set severity.

#### Set Status

Select to set status.

#### Run Smart Response

Select to run a Smart Response rule you or your administrator configured.

See "Discover incident lists" on page 995.

## **Network Discover incident entries**

Incident information is divided into several columns.

Click any column header to sort alpha-numerically by that column's data. To sort in reverse order, click the column header a second time.

The report includes the following columns:

Check boxes that let you select incidents to remediate.

You can select one or more incidents to which to apply commands from the Incident Actions drop-down menu.

Click the checkbox at the top of the column to select all incidents on the current page.

You can click **Select All** at far right to select all incidents in the report.

Note: Use caution when you use Select All. This option selects all incidents in the report (not only those on the current page), and any incident command you subsequently apply affects all incidents. You may want to configure the maximum-incident-batch-size property to limit the number of incidents that a Server FlexResponse plug-in processes at one time.

See "Adding a Server FlexResponse plug-in to the plug-ins properties file" on page 1232.

#### Type

Type of target in which the match was detected.

An icon represents each target type.

This column also displays a remediation icon, if any response rule applied.

The possible values are as follows:

Blank if no response rule applied

Copied m

Quarantined

Remediation Error

When you use a Server FlexResponse action for an Automated or Smart response rule, one of the following icons may appear:

- **₽** This incident was successfully remediated using a Server FlexResponse action.
- The Server FlexResponse action is in process.
- The Server FlexResponse action has an error.

These same icons may appear for other incident types as well, and you can execute Server FlexResponse actions on those incidents.

See "Configuring the Server FlexResponse action" on page 912.

- Location/Target/Scan Repository or file location, target name, and date and time of most recent scan
- File Owner Username of file owner (for example, MYDOMAIN\Administrator)
- ID/Policy

Symantec Data Loss Prevention incident number and the policy against which the incident was logged

Matches

Number of matches in the incident

Severity

Incident severity as determined by the severity setting of the rule the incident matched

The possible values are as follows:

- Ш High
- Medium
- Low
- For information only 111

#### Status

Current incident status

The possible values are as follows:

- New
- In Process
- Escalated
- False Positive
- **Configuration Errors**
- Resolved

The following icon may be displayed near the status if this incident was seen before:

This icon is displayed if this incident has an earlier connected incident. 

You or your administrator can add new status designations on the attribute setup page.

See "Configuring custom attributes" on page 1079.

See "Discover incident lists" on page 995.

## **Discover summary reports**

Discover Summary Reports provide summary information about the incidents that are found during Discover scans.

If you are running Endpoint Discover, the Discover Summary Reports also include Endpoint Discover incidents.

You can filter or summarize the options in the reports.

See "Incident report filter and summary options" on page 1040.

You can extract the report information in selected formats.

You can click highlighted elements, such as the entries in the Totals column, to drill down into details.

Icons provide navigation through long reports.

See "Page navigation in incident reports" on page 1039.

See "Discover incident reports" on page 990.

# Working with Classification incidents

This chapter includes the following topics:

- Classification incident list
- Classification incident snapshot

## Classification incident list

The Classification incident list applies only to deployments where the Symantec Data Classification for Enterprise Vault solution is deployed. This solution uses Symantec Data Loss Prevention to classify email messages and forward them to Symantec Enterprise Vault for archiving or other actions. The solution is licensed separately from Symantec Data Loss Prevention. Classification incidents display in the Classification incident list only when a message violates a policy that is configured with the **Enable Classification Test Mode** option enabled. Classification test mode is used only to verify policy matches. During normal production operations, Classification test mode should be disabled.

See "About implementing detection for Enterprise Vault Classification" on page 620.

Table 45-1 describes the columns that display in the Classification incident list.

**Table 45-1** Classification incident list columns

Column	Definition
Туре	The <b>Type</b> column displays the icons that identify the incident as a classification email incident. An additional icon also displays when the email has an attachment.

**Table 45-1** Classification incident list columns (continued)

Column	Definition
Subject/Sender/Recipient(s)	Displays the sender, subject line, and recipient list of the email.
Sent	Displays the date and time the email was sent.
ID/Policy	Symantec Data Loss Prevention incident ID number and the policy against which the incident was logged.
Matches	Number of matches in the incident.
Severity	Incident severity as determined by the severity setting of the rule the incident matched.  The possible values are as follows:  High Medium Low For information only
Status	Current incident status  The possible values are as follows:  New In Process Escalated False positive Configuration Errors Resolved  You or your administrator can add new status designations on the Attribute Setup page.

# Classification incident snapshot

A Classification incident snapshot provides detailed information about a particular incident. It displays general incident information, matches detected in the intercepted text, and details about attributes, incident history, and the violated policy. You can also search for similar incidents in the Correlations area.

Classification test mode is used only to verify policy matches. During normal production operations, Classification test mode should be disabled.

See "Classification incident list" on page 1000.

Current status and severity appear under the snapshot heading. To change one of the current values, click on it and choose another value from the drop-down list. If any action icon is associated, it also appears here.

Table 45-2 describes the incident the information that is presented in the snapshot.

Table 45-2 Incident general information tabs

Table 45-2	incident general information tabs	
Tab Name	Description	
Key Info	The Key Info tab shows the policy that was violated in the incident. It also shows the total number of matches for the policy, as well as matches per policy rule. Click the policy name to view a list of all incidents that violated the policy. Click <b>view policy</b> to view a read-only version of the policy.	
	This section also lists other policies that the same file violated. To view the snapshot of an incident that is associated with a particular policy, click <b>go to incident</b> next to the policy name. To view a list of all incidents that the file created, click <b>show all</b> .	
	The Key Info tab also includes the following information:	
	<ul> <li>The name of the detection server that recorded the incident.</li> <li>The date and time the message was sent</li> <li>The sender email or IP address</li> <li>The recipient email or IP address(es)</li> <li>The SMTP heading or the NNTP subject heading</li> <li>The Is Archived field displays the archived state of the incident and whether or not the incident is archivable. It also lets you toggle the Do Not Archive flag for the incident.</li> <li>Attachment file name(s). Click to open or save the file. If a response rule tells Symantec Data Loss Prevention to discard the original message, you cannot view the attachment.</li> </ul>	
History	View the actions that were performed on the incident. For each action, Symantec Data Loss Prevention displays the action date and time, the actor (a user or server), and the action or the comment.	

Table 45-2 Incident general information tabs (continued)

Tab Name	Description
Notes	View any notes that you or others have added to the incident. Click <b>Add Note</b> to add a note.
Correlations	You can view a list of those incidents that share attributes of the current incident. For example, you can view a list of all incidents that a single account generated. The <b>Correlations</b> tab shows a list of correlations that match single attributes. Click on attribute values to view lists of those incidents that are related to those values.
	To search for other incidents with the same attributes, click Find Similar. In the Find Similar Incidents dialog box that appears, select the desired search attributes. Then click Find Incidents.  Note: The list of correlated incidents does not display related incidents that have been archived.

Beneath the general information, Symantec Data Loss Prevention displays the message content (if applicable) and the matches that caused the incident.

Matches are highlighted in yellow and organized according to the message component (such as header, body, or attachment) in which they were detected. Symantec Data Loss Prevention displays the total relevant matches for each message component. It shows matches by the order in which they appear in the original text. To view the rule that triggered a match, click on the highlighted match.

# Managing and reporting incidents

#### This chapter includes the following topics:

- About Symantec Data Loss Prevention reports
- About strategies for using reports
- Setting report preferences
- About incident reports
- About dashboard reports and executive summaries
- Viewing dashboards
- Creating dashboard reports
- Configuring dashboard reports
- Choosing reports to include in a dashboard
- About summary reports
- Viewing summary reports
- Creating summary reports
- Viewing incidents
- About custom reports and dashboards
- Using IT Analytics to manage incidents
- Filtering reports

- Saving custom incident reports
- Scheduling custom incident reports
- Delivery schedule options for incident and system reports
- Delivery schedule options for dashboard reports
- Using the date widget to schedule reports
- Editing custom dashboards and reports
- **Exporting incident reports**
- Exported fields for Network Monitor
- Exported fields for Network Discover
- Exported fields for Mobile Prevent for Web
- Exported fields for Endpoint Discover
- **Deleting incidents**
- Deleting custom dashboards and reports
- Common incident report features
- Page navigation in incident reports
- Incident report filter and summary options
- Sending incident reports by email
- Printing incident reports
- Incident snapshot history tab
- Incident snapshot attributes section
- Incident snapshot correlations tab
- Incident snapshot policy section
- Incident snapshot matches section
- Incident snapshot access information section
- Customizing incident snapshot pages
- About filters and summary options for reports
- General filters for reports

- Summary options for incident reports
- Advanced filter options for reports

## **About Symantec Data Loss Prevention reports**

Use incident reports to track and respond to incidents. Symantec Data Loss Prevention reports an incident when it detects data that matches the detection parameters of a policy rule.

Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information.

Each piece of data that matches detection parameters is called a match, and a single incident may include any number of individual matches.

You can set an incident archive flag on an incident to indicate that the incident has been archived. By default, archived incidents do not appear in incident reports, but you can include them in incident reports by setting Advanced Filters on the report. Including archived incidents in a report may slow down reporting activities. See "About incident archiving" on page 1065.

Symantec Data Loss Prevention tracks incidents for all detection servers. These servers include Network Discover Server, Network Monitor Server, Network Prevent for Email Server, Network Prevent for Web Server, Mobile Prevent for Web Server, and Endpoint Server.

You can specify the reports Symantec Data Loss Prevention displays in the navigation panel.

See "Setting report preferences" on page 1008.

Symantec Data Loss Prevention provides the following types of incident reports:

- Incident lists show the individual incident records that contain information such as severity, associated policy, number of matches, and status. You can click on any incident to see a snapshot containing more details. And you can select specific incidents or groups of incidents to modify or remediate. Symantec Data Loss Prevention provides separate reports for incidents by selecting Network, Endpoint, Mobile, Discover, or User.
- Summaries provide summary information about the incidents on your system. They are organized with either one or two summary criteria. A single-summary report is organized with a single summary criterion, such as the policy that is associated with each incident. A double-summary report is organized with two criteria, such as policy and incident status. By default, archived incidents do not appear in the counts that display in summary reports, but you can set Advanced

Filters to include the archived incidents. (See "About incident archiving" on page 1065.)

 Dashboards combine information from several reports. They include graphs and incident totals representing the contents of various incident lists and summaries. Graphs can sometimes contain lists of high-severity incidents or lists of summary groups. You can click on report portlets (the individual tiles that contain report data) to drill down to the detailed versions of the reports.

Symantec Data Loss Prevention ships with executive summaries for **Network**, Endpoint, Mobile, and Discover incidents.

Executive summaries are very similar to dashboards. The difference between them is that you can customize a dashboard, but you cannot customize an executive summary.

You can create and save customized versions of all reports (except executive summaries) for continued use.

See "About custom reports and dashboards" on page 1019.

Symantec Data Loss Prevention displays reports in separate sections on the Incident Reports screen as follows:

- The **Saved Reports** section contains any shared reports that are associated with your current role. This section appears only if you or other users in your current role have created saved reports.
  - See "About custom reports and dashboards" on page 1019.
- The **Network** section contains Symantec-provided incident lists, summaries, and dashboards for network incidents.
- The Mobile section contains Symantec-provided incident lists, summaries, and dashboards for mobile incidents.
- The **Endpoint** section contains Symantec-provided incident lists, summaries, and dashboards for endpoint incidents. Endpoint reports include the incidents that Endpoint captures, such as Endpoint Block and Endpoint Notify incidents. Incidents that Endpoint Discover captures appear in Discover reports.
- The **Discover** section contains Symantec-provided incident lists, summaries, and dashboards for Network Discover and Endpoint Discover incidents.
- The Users section contains the user list and user risk summary, which displays users and their associated Email and Endpoint incidents.

## About strategies for using reports

Many companies configure their Symantec Data Loss Prevention reporting to accommodate the following primary roles:

An executive responsible for overall risk reduction who monitors risk trends and develops high-level initiatives to respond to those trends.

The executive monitors dashboards and summary reports (to get a general picture of data loss trends in the organization). The executive also develops programs and initiatives to reduce risk, and communicates this information to policy authors and incident responders. The executive often monitors reports through email or some other exported report format.

Symantec Data Loss Prevention dashboards and summary reports let you monitor risk trends in your organization. These reports provide a high-level overview of incidents. Executives and managers can guickly evaluate risk trends and advise policy authors and incident responders how to address these trends. You can view existing summary reports and dashboards and create customized versions of these reports.

See "About dashboard reports and executive summaries" on page 1011. See "About summary reports" on page 1016.

 An incident responder, such as an InfoSec Analyst or InfoSec Manager, who monitors and responds to particular incidents.

The responder monitors incident reports and snapshots to respond to the incidents that are associated with a particular policy group, organizational department, or geographic location. The responder may also author policies to reduce risk. These policies can originate either at the direction of a risk reduction manager or based on their own experience tracking incidents.

See "About incident remediation" on page 940.

## Setting report preferences

You can specify the reports that Symantec Data Loss Prevention displays in the navigation panel for each of the report types.

#### To set reporting preferences

- In the Enforce Server administration console, on the Incidents menu, click All Reports.
- 2 On the All Reports screen, click Edit Preferences.

The Edit Report Preferences screen lists any saved reports (for all your assigned roles).

The screen also lists Network, Endpoint, Mobile, and Discover reports.

3 To display a report in the list, check the **Show Report** box for that report. To remove a report from the list, clear **Show Report** for that report.

The selected list of reports displays in a left navigation panel for each of the types of reports.

For example, to see the list of Network reports, on the **Incidents** menu, click Network.

After changing your preferences, click **Save**.

See "About custom reports and dashboards" on page 1019.

### About incident reports

Use incident reports to track and respond to incidents on your network. Symantec Data Loss Prevention reports an incident when it detects data that matches a detection rule in an active policy. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches a detection rule is called a match, and a single incident may include any number of individual matches.

Note: You can configure which reports appear in navigation panel. To do so, go to All Reports and then click on Edit Preferences

Symantec Data Loss Prevention provides the following types of incident reports:

Incident lists These show individual incident records containing information such as

> severity, associated policy, number of matches, and status. You can click on any incident to view a snapshot containing more details. You can select specific incidents or groups of incidents to modify or remediate.

Summaries These show incident totals organized by a specific incident attribute such

> as status or associated policy. For example, a **Policy Summary** includes rows for all policies that have associated incidents. Each row includes a policy name, the total number of associated incidents, and incident totals by severity. You can click on any severity total to view the list of relevant

incidents.

Double summaries These show incident totals organized by two incident attributes. For example, a policy trend summary shows the total incidents by policy and by week. Similar to the policy summary, each entry includes a policy name, the total number of associated incidents, and incident totals by severity. In addition, each entry includes a separate line for each week, showing the week's incident totals and incidents by severity.

executive summaries

Dashboards and These are quick-reference dashboards that combine information from several reports. They include graphs and incident totals representing the contents of various incident lists, summaries, and double summaries. Graphs are sometimes beside lists of high-severity incidents or lists of

summary groups. You can click on constituent report names to drill down

to the reports that are represented on the dashboard.

Symantec Data Loss Prevention ships with executive summaries for Network, Endpoint, and Discover reports, and these are not customizable.

You can create dashboards yourself, and customize them as desired.

Custom Lists the shared reports that are associated with your current role. (Such

reports appear only if you or other users in your current role have created

them.)

Network Lists the network incident reports.

**Endpoint** Lists the Endpoint incident reports. Endpoint reports include incidents

such as Endpoint Block and Endpoint Notify incidents.

Incidents from Endpoint Discover are included in Discover reports.

Discover Lists Network Discover and Endpoint Discover incident reports.

> The folder risk report displays file share folders ranked by prioritized risk. The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the VML

Management Server.

See the Symantec Data Loss Prevention Data Insight Implementation

Guide

Mobile Lists Mobile Prevent for Web incident reports.

Users The User List lists the data users in your organization. The User Risk

Summary lists all users with their associated Email and Endpoint incidents.

See "About custom reports and dashboards" on page 1019.

See "Common incident report features" on page 1039.

See "Network incident snapshot" on page 956.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Mobile incident snapshot" on page 978.

See "Network incident list" on page 950.

See "Discover incident lists" on page 995.

See "Endpoint incident lists" on page 964.

See "Mobile incident variables" on page 947.

### About dashboard reports and executive summaries

Dashboards and executive summaries are the quick-reference report screens that present summary information from several incident reports.

Symantec Data Loss Prevention ships with one executive summary each for Network, Endpoint, Mobile, and Discover incident reports.

See "About incident reports" on page 1009.

Dashboards and executive summaries have two columns of reports. The left column displays a pie chart or graph and an incident totals bar. The right column displays the same types of information as in the left column. The right column also displays either a list of the most significant incidents or a list of summary items with associated incident totals. The most significant incidents are ranked using severity and match count. You can click on a report to see the full report it represents.

Dashboards consist of up to six portlets, each providing a quick summary of a report you specify.

Symantec Data Loss Prevention includes three executive summaries (which are similar to dashboards): Executive Summary-Network, Executive Summary-Endpoint, Executive Summary-Mobile, and Executive Summary-Discover. (Dashboards and executive summaries share the same format, but executive summaries are not customizable.)

You can create customized dashboards for users with specific security responsibilities. If you choose to share a dashboard, the dashboard is accessible to all users in the role under which you create it. (Note that the Administrator user cannot create shared dashboards.)

Dashboards have two columns of report portlets (tiles that contain report data). Portlets in the left column display a pie chart or graph and the totals bar. Portlets in the right column display the same types of information as those in the left. However, they also display either a list of the most significant incidents or a list of summary criteria and associated incidents. The incidents are ranked using severity and match count. The summary criteria highlights any high-severity incident totals. You can choose up to three reports to include in the left column and up to three reports to include in the right column.

To create custom dashboards, click Incident Reports at the top of the navigation panel and, in the Incident Reports screen that appears, click Create Dashboard. The Administrator can create only private dashboards, but other users can decide whether to share a new dashboard or keep it private.

See "About custom reports and dashboards" on page 1019.

To edit the contents of any custom dashboard, go to the desired dashboard and click **Customize** near the top of the screen.

See "Configuring dashboard reports" on page 1014.

To display a custom dashboard at logon, specify it as the default logon report.

See "Setting report preferences" on page 1008.

### Viewing dashboards

This procedure shows you how to view a dashboard.

#### To view a dashboard

In the Enforce Server administration console, on the Incidents menu, click **Incident Reports**. Under **Reports**, click the name of a dashboard.

Dashboards consist of up to six portlets that each provide a summary of a particular report.

For example, the **Executive Summary-Network** dashboard consists of portlets for the Network Policy Summary, High Risk Senders, Protocol Summary, Top Recipient Domains, Status by Week, and Incidents - All.

- To see the entire report for a portlet, click the portlet.
  - Symantec Data Loss Prevention displays the appropriate incident list or summary report.
- 3 Browse through the incident list or summary report.

See "Viewing incidents" on page 1018.

See "About summary reports" on page 1016.

### Creating dashboard reports

You can create custom dashboards and reports.

If you are logged on as a user other than the administrator, Symantec Data Loss Prevention lets you choose whether to share your dashboard or keep it private.

#### To create a dashboard

- In the Enforce Server administration console, on the Incidents menu, click Incident Reports.
- 2 On the **Incident Reports** screen that appears, click **Create Dashboard**. The Configure Dashboard screen appears.
- 3 Choose whether to share your dashboard or keep it private.

If you choose to share a dashboard, the dashboard is accessible to all users assigned the role under which you create it.

If you are logged on as Administrator, you do not see this choice.

Note: Symantec Data Loss Prevention automatically designates all dashboards that the administrator creates as private.

Click Next.

- 4 In the **General** section, for **Name**, type a name for the dashboard.
- 5 For **Description**, type an optional description for the dashboard.
- In the **Delivery Schedule** section, you can regenerate and send the dashboard report to specified email accounts.

If SMTP is not set up on your Enforce Server, you do not see the Delivery Schedule section.

If you have configured your system to send alerts and reports, you can set a time to regenerate and send the dashboard report to specified email accounts.

See "Configuring the Enforce Server to send email alerts" on page 146.

If you have not configured Symantec Data Loss Prevention to send reports, skip to the next step.

To set a schedule, locate the **Delivery Schedule** section and select an option from the **Schedule** drop-down list. (You can alternatively select **No Schedule**.)

For example, select **Send Weekly On**.

Enter the data that is required for your **Schedule** choice. Required information includes one or more email addresses (separated by commas). It may also include calendar date, time of day, day of the week, day of the month, or last date to send.

See "Delivery schedule options for dashboard reports" on page 1027.

For the **Left Column**, you can choose what to display in a pie chart or graph. For the **Right Column**, you can also display a table of the information.

See "Choosing reports to include in a dashboard" on page 1015.

Select a report from as many as three of the Left Column (Chart Only) drop-down lists. Then select a report from as many as three of the Right Column (Chart and Table) drop-down lists.

- Click Save.
- You can edit the dashboard later from the **Edit Report Preferences** screen.

To display a custom dashboard at logon, specify it as the default logon report on the Edit Report Preferences screen.

See "Editing custom dashboards and reports" on page 1029.

# Configuring dashboard reports

You can create the custom dashboards that are tailored for users with specific roles.

Dashboards consist of up to six portlets, each providing a guick summary of a report you specify.

If you choose to share a dashboard, the dashboard is accessible to all users assigned the role under which you create it.

**Note:** The Administrator user cannot create shared dashboards.

### To configure a custom dashboard

- In the **General** section, for **Name**, type a name for the dashboard. 1
- 2 For **Description**, type an optional description for the dashboard.

3 In the **Delivery Schedule** section, you can regenerate and send the dashboard report to specified email accounts.

If SMTP is not set up on your Enforce Server, you do not see the **Delivery** Schedule section.

If you have configured your system to send alerts and reports, you can set a time to regenerate and send the dashboard report to specified email accounts.

See "Configuring the Enforce Server to send email alerts" on page 146.

If you have not configured Symantec Data Loss Prevention to send reports, skip to the next step.

To set a schedule, locate the **Delivery Schedule** section and select an option from the **Schedule** drop-down list. (You can alternatively select **No Schedule**.)

For example, select Send Weekly On.

Enter the data that is required for your **Schedule** choice. Required information includes one or more email addresses (separated by commas). It may also include calendar date, time of day, day of the week, day of the month, or last date to send.

See "Delivery schedule options for dashboard reports" on page 1027.

For the **Left Column**, you can choose what to display in a pie chart or graph. For the **Right Column**, you can also display a table of the information.

See "Choosing reports to include in a dashboard" on page 1015.

Select a report from as many as three of the Left Column (Chart Only) drop-down lists. Then select a report from as many as three of the Right Column (Chart and Table) drop-down lists.

- Click Save. 5
- You can edit the dashboard later from the **Edit Report Preferences** screen.

To display a custom dashboard at logon, specify it as the default logon report on the Edit Report Preferences screen.

See "Editing custom dashboards and reports" on page 1029.

### Choosing reports to include in a dashboard

Dashboards have two columns of report portlets.

Portlets in the left column display a pie chart or graph.

Portlets in the right column display the same information as those in the left. They also display either a list of the most significant incidents or a summary. Incidents

are ranked with severity and match count. You can display a list of summary criteria and associated incidents that highlight any high-severity incident totals.

You can choose up to three reports to include in the left column, and up to three reports to include in the right column.

#### To choose reports to include

- Choose a report from as many as three of the **Left Column (Chart Only)** drop-down lists.
- 2 Choose a report from as many as three of the Right Column (Chart and Table) drop-down lists.
- After you configure the dashboard, click Save.

See "Configuring dashboard reports" on page 1014.

### **About summary reports**

Symantec Data Loss Prevention provides two types of summary reports: single summaries and double summaries.

Single summaries show incident totals organized by a specific incident attribute such as status or associated policy. For example, a policy summary includes a row for each policy that has associated incidents. Each row includes a policy name, the total number of associated incidents, and incident totals by severity.

Double summaries show incident totals organized by two incident attributes. For example, a policy trend summary shows the total incidents which are organized with policy and week. As in a policy summary, each entry includes a policy name, the total number of associated incidents, and incident totals by severity. In addition, each entry includes a separate line for each week, showing the week's incident totals and incidents by severity.

See "Summary options for incident reports" on page 1051.

You can create custom summary reports from any incident list.

## Viewing summary reports

This procedure shows you how to view a summary report.

#### To view a summary report

In the Enforce Server administration console, on the Incidents menu, select one of the types of reports.

For example, select **Network**, and then click **Policy Summary**.

The report consists of summary entries (rows) that are divided into several columns. The first column is named for the primary summary criterion. It lists primary and (for double summaries) secondary summary items. For example, in a **Policy Summary** this column is named **Policy** and it lists policies. Each entry includes a column for total number of associated incidents. It also includes columns showing the number of incidents of High, Medium, Low, and Informational severity. Finally, it includes a bar chart that represents the number of incidents by severity.

- Optionally, you can sort the report alpha-numerically by a particular column's data. To do so, click the wanted column heading. To sort in reverse order, click the column heading a second time.
- 3 To identify areas of potential risk, click the High column heading to display summary entries by number of high-severity incidents.
- Click an entry to see a list of associated incidents. In any of the severity columns, you can click the total to see a list of incidents of the chosen severity. See "Viewing incidents" on page 1018.

### **Creating summary reports**

This procedure shows you how to create a summary report.

### To create a summary report from an incident list

- In the Enforce Server administration console, on the Incidents menu, select one of the types of reports, and then click an incident list.
  - For example, select **Discover**, and then the report **Incidents-All Scans**.
- 2 Click the Advanced Filters & Summarization bar (near the top of the report).
  - In **Summarize By** for the primary listbox and secondary listbox that appear. Symantec Data Loss Prevention displays all Symantec-provided criteria in alphabetical order. The criteria precedes any custom criteria the administrator has defined.

See "Summary options for incident reports" on page 1051.

- 3 Select a criterion from the primary listbox, and an optional criterion from the secondary listbox. For example, select Policy Group and then Policy. (Note that options in the secondary listbox appear only after you choose an option from the primary listbox.)
- 4 To create the summary report, click **Apply**.
  - Summary reports take their name from the primary summary criterion. If you rerun a report with new criteria, the report name changes accordingly.
- 5 Save the report.

See "Saving custom incident reports" on page 1022.

### Viewing incidents

Symantec Data Loss Prevention incident lists display the individual incident records with information about the incidents. You can click on any incident to see a snapshot containing more details. You can select specific incidents or groups of incidents to modify or remediate.

Symantec Data Loss Prevention provides incident lists for Network, Endpoint, and Discover incidents.

#### To view incidents

In the Enforce Server administration console, on the **Incidents** menu, select one of the types of reports.

For example, select **Discover**. In the left navigation panel, click **Incidents-All** Scans.

The incident list displays the individual incident records that contain information such as severity, associated policy, number of matches, and status.

2 Optionally, use report filters to narrow down the incident list.

See "Filtering reports" on page 1021.

3 To view more details of a particular incident, click the incident.

The incident snapshot appears, displaying general incident information, matches detected in the intercepted text, and details about policy, attributes, and incident history.

You can also search for similar incidents from the **Correlations** tab.

Optionally, click through the incident snapshot to view more information about the incident.

The following list describes the ways you can access more information through the snapshot:

- You can find information about the policy that detected the incident. On the Key Info tab, the Policy Matches section displays the policy name. Click on the policy name to see a list of incidents that are associated with that policy. Click view policy to see a read-only version of the policy. This section also lists other violated policies with the same file or message. When multiple policies are listed, you can see the snapshot of an incident that is associated with a particular policy. Click go to incident next to the policy name. To see a list of all incidents that the file or message created, click show all.
- You can view lists of the incidents that share various attributes with the current incident. The **Correlations** tab shows a list of correlations that match single attributes. Click on attribute values to see the lists of incidents that are related to those values.
  - For example, the current network incident is triggered from a message from a particular email account. You can bring up a list of all incidents that this account created.
- For most network incidents, you can access any attachments that are associated with the network message. To do so, locate the **Attachments** field in the Incident Details section of the snapshot and click the attachment file name.

For a detailed description of incident snapshots and the actions you can perform through them, see the online Help.

When you finish viewing incidents, you can exit the incident snapshot or incident list, or you can choose one or more incidents to remediate.

See "Remediating incidents" on page 943.

### About custom reports and dashboards

You can filter and summarize reports, and then save them for continued use. When saving a customized report, you can configure Symantec Data Loss Prevention to send the report according to a specific schedule.

Symantec Data Loss Prevention displays the titles of customized reports under Incidents > Incident Reports.

The **Incident Reports** screen displays all out-of-the-box and custom reports available to your assigned role(s). The list includes shared custom reports and the dashboards that you or anyone else in your current role created. Several standard reports are available with Symantec Data Loss Prevention.

Symantec Data Loss Prevention displays each report's name, associated product, and description. For custom reports, Symantec Data Loss Prevention indicates

whether the report is shared or private and displays the report generation and delivery schedule.

You can modify existing reports and save them as custom reports, and you can also create custom dashboards. Custom reports and dashboards are listed in the **Saved Reports** section of the navigation panel.

You can click any report on the list to re-run it with current data.

You can view and run custom reports for reports created by users who have any of the roles that are assigned to you. You can only edit or delete the custom reports that are associated with the current role. The only custom reports visible to the Administrator are the reports that the Administrator user created.

A set of tables lists all the options available for filtering and summarizing reports.

See "About summary reports" on page 1016.

See "Summary options for incident reports" on page 1051.

See "General filters for reports" on page 1047.

See "Advanced filter options for reports" on page 1056.

Create Dashboard Lets you create a custom dashboard that displays summary data from several reports you specify. For users other than the Administrator, this option leads to the Configure Dashboard screen, where you specify whether the dashboard is private or shared. All Administrator dashboards are private.

See "Creating dashboard reports" on page 1012.

Edit Preferences Lets you specify the report that displays at logon, as well as the reports that should appear in the navigation panel.

See "Editing custom dashboards and reports" on page 1029.

Saved (custom) reports associated with your role appear near the top of the screen.

The following options are available for your current role's custom reports:

Click this icon next to a report to display the save report or configure dashboard screen. You can change the name, description, or schedule, or (for dashboards only) change the reports to include.

See "Saving custom incident reports" on page 1022.

See "Configuring dashboard reports" on page 1014.

1 Click this icon next to a report to display the screento change the scheduling of this report. If this icon does not display, then this report is not currently scheduled.

See "Saving custom incident reports" on page 1022.

Click this icon next to a report to delete that report. A dialog prompts you to confirm the deletion. When you delete a report, you cannot retrieve it. Make sure that no other role members need the report before you delete it.

### Using IT Analytics to manage incidents

IT Analytics Solution is a Business Intelligence (BI) application that complements and expands upon the reporting that is offered by Symantec Data Loss Prevention. It provides multi-dimensional analysis and robust graphical reporting features to Symantec Management Platform. This functionality lets you create on-the-fly ad-hoc reports without advanced knowledge of databases or third-party reporting tools. IT Analytics provides this powerful on-the-fly ad-hoc reporting with pivot tables, precompiled aggregations for fast answers to typically long-running queries, and easy export to .PDF, Excel, .CSV and .TIF files.

The IT Analytics Solution is supported for Symantec Data Loss Prevention version 10.5 and later.

For more information, see the Data Loss Prevention Pack for Altiris IT Analytics Solution 7.1 SP2 from Symantec User Guide, available at the following URL:

http://www.symantec.com/business/support/index?page=content&id=DOC5526&key=56005

### Filtering reports

You can filter an incident list or summary report.

#### To filter an incident list

- In the Enforce Server administration console, on the Incidents menu, select one of the types of reports.
  - For example, select **Network**, and then click **Policy Summary**.
- 2 In the Filter area, current filters are displayed, as well as options for adding and running other filters.

- Modify the default filters as wanted. For example, from the **Status** filter drop-down lists, select Equals and New.
  - For Network, Mobile, and Endpoint reports, the default filters are **Date** and Status. For Discover reports, default filters are Status, Scan, and Target ID.
- To add a new filter, select filter options from the drop-down lists. Click Advanced Filters & Summarization for additional options. Click Add Filter on the right, for additional filter options.
  - Select the filter type and parameters from left to right as if writing a sentence. For example, from the advanced filters, Add Filter options, select Policy and Is Any Of, and then select one or more policies to view in the report. Hold down Ctrl or Shift to select more than one item in the listbox.
- 5 Click **Apply** to update the report.
- 6 Save the report.

See "Saving custom incident reports" on page 1022.

## Saving custom incident reports

After you summarize or filter a report, you can save it for continued use. When you save a customized report, Symantec Data Loss Prevention displays the report title under Saved Reports in the Incident Reports section. If a user chooses to share the report, Symantec Data Loss Prevention displays the report link only for users who belong to the same role as the user who created the report.

See "About custom reports and dashboards" on page 1019.

You can edit the report later on the Edit Preferences screen.

See "Editing custom dashboards and reports" on page 1029.

Optionally, you can schedule the report to be run automatically on a regular basis.

See "Scheduling custom incident reports" on page 1023.

#### To save a custom report

Set up a customized filter or summary report.

See "About custom reports and dashboards" on page 1019.

Click Save > Save As.

2 Enter a unique report name and describe the report. The report name can include up to 50 characters.

3 In the **Sharing** section, users other than the administrator can share a custom report.

**Note:** This section does not appear for the administrator.

The **Sharing** section lets you specify whether to keep the report private or share it with other role members. Role members are other users who are assigned to the same role. To share the report, select **Share Report**. All role members now have access to this report, and all can edit or delete the report. If your account is deleted from the system, shared reports remain in the system. Shared reports are associated with the role, not with any specific user account. If you do not share a report, you are the only user who can access it. If your account is deleted from the system, your private reports are deleted as well. If you log on with a different role, the report is visible on the **Incident Reports** screen, but not accessible to you.

Click Save.

# Scheduling custom incident reports

Optionally, you can schedule a saved report to be run automatically on a regular basis.

You can also schedule the report to be emailed to specified addresses or to the data owners on a regular schedule.

See the Symantec Data Loss Prevention Data Insight Implementation Guide.

### To schedule a custom report

1 Click Send > Schedule Distribution.

If SMTP is not set up on your Enforce Server, you are not able to select the Send menu item to send the report.

See "Configuring the Enforce Server to send email alerts" on page 146.

2 Specify the **Delivery Details**:

То:	Select whether the report is sent to specified email addresses or to the data owners.
Manual - Sent to specified e-mail addresses	Enter the specific email addresses manually in the text box.
Auto - Send to incident data owners	To send the report to the data owners, the <b>Send report data with emails</b> setting must be enabled for this option to appear.
	See "Configuring the Enforce Server to send email alerts" on page 146.
	If you select to have the report sent to the incident data owners, then the email address in the incident attribute <b>Data</b> Owner Email Address is the address where the report is sent.
	This <b>Data Owner Email Address</b> must be set manually, or with a lookup plug-in.
	See the Symantec Data Loss Prevention Data Insight Implementation Guide.
	A maximum of 10000 incidents can be distributed per data owner.
CC:	Enter the email addresses manually in the text box.
Subject:	Use the default subject or modify it.
Body:	Enter the body of the email.
	Response action variables can also be entered in the body.
	See "Response action variables"

on page 946.

In the **Schedule Delivery** section, specify the delivery schedule.

See "Delivery schedule options for incident and system reports" on page 1025.

In the Change Incident Status / Attributes section, you can implement workflow.

The Auto - Send to incident data owners option must be set for this section to appear.

See "Configuring the Enforce Server to send email alerts" on page 146.

- 5 After sending the report, you can change an incident's status to any of the valid values. Select a status value from the drop-down list.
- You can also enter new values for any custom attributes.

These attributes must be already set up.

See "About incident status attributes" on page 1069.

- 7 Select one of the custom attributes from the drop-down list.
- 8 Click Add.
- In the text box, enter the new value for this custom attribute.

After sending the report, the selected custom attributes set the new values for those incidents that were sent in the report.

- 10 Click Next.
- 11 Enter the name and description of the saved report.
- 12 Click Save.

# Delivery schedule options for incident and system reports

The **Schedule Delivery** section lets you set up a schedule for the report.

Note: If your Enforce Server is not configured to send email, or you are not allowed to send reports, the **Schedule Delivery** section does not appear.

When you make a selection from the list, additional fields appear.

To remove scheduling of a report that was previously scheduled, click the Remove option.

The following table describes the additional fields available for each option on the list.

#### **Delivery Details**

Specify the following delivery details:

#### Send To

Specify Manual to specify the email addresses. Specify Auto for automatic sending to data owners.

#### To

Enter one or more email addresses. Separate them with commas.

Enter one or more email addresses. Separate them with commas.

#### Subject

Provide a subject for the email.

#### Body

Enter the body of the email. Use variables for items such as the policy name.

See "Response action variables" on page 946.

#### One time

Select **One time** to schedule the report to be run once at a future time, and then specify the following details for that report:

#### Time

Select the time you want to generate the report.

#### Send Date

Enter the date you want to generate the report, or click the date widget and select a date.

### Daily

Select Daily to schedule the report to be run every day, and then specify the following details for that report:

#### Time

Select the time you want to generate the report.

#### Until

Enter the date you want to stop generating daily reports, click the date widget and select a date, or select Indefinitely.

#### Weekly

Select Weekly on to schedule the report to be run every week, and then specify the following details for that report:

#### ■ Time

Select the time you want to generate the report.

#### Days of Week

Click to check one or more check boxes to indicate the day(s) of the week you want to generate the report.

#### Until

Enter the date you want to stop generating weekly reports, click the date widget and select a date, or select Indefinitely.

#### Monthly

Select Monthly on to schedule the report to be run every month, and then specify the following details for that report:

Time

Select the time you want to generate the report.

Day of Month

Enter the date on which you want to generate the report each month.

Until

Enter the date you want to stop generating monthly reports, click the date widget and select a date, or select Indefinitely.

See "Saving custom incident reports" on page 1022.

See "Working with saved system reports" on page 138.

### Delivery schedule options for dashboard reports

The **Delivery Schedule** section lets you set up a schedule for the report.

Note: If your Enforce Server is not configured to send email, or you are not allowed to send reports, the **Delivery Schedule** section does not appear.

When you make a selection from the **Schedule** drop-down list, additional fields appear.

The following table describes the additional fields available for each option on the list.

No Schedule

Select No Schedule to save the report without a schedule.

Once

Select Once to schedule the report to be run once at a future time, and then specify the following details for that report:

Enter the date you want to generate the report, or click the date widget and select a date.

At

Select the time you want to generate the report.

Send To

Enter one or more email addresses. Separate them with commas.

#### **Send Every Day**

Select **Send Every Day** to schedule the report to be run every day, and then specify the following details for that report:

At

Select the time you want to generate the report.

Enter the date you want to stop generating daily reports, click the date widget and select a date, or select Indefinitely.

Send To

Enter one or more email addresses. Separate them with commas.

#### Send Weekly On

Select Send Weekly on to schedule the report to be run every week, and then specify the following details for that report:

Day

Click to check one or more check boxes to indicate the day(s) of the week you want to generate the report.

At

Select the time you want to generate the report.

Until

Enter the date you want to stop generating weekly reports, click the date widget and select a date, or select Indefinitely.

Send To

Enter one or more email addresses. Separate them with commas.

Send Monthly On Select Send Monthly on to schedule the report to be run every month, and then specify the following details for that report:

Day of each month

Enter the date on which you want to generate the report each month.

At

Select the time you want to generate the report.

Until

Enter the date you want to stop generating monthly reports, click the date widget and select a date, or select Indefinitely.

Send To

Enter one or more email addresses. Separate them with commas.

See "Configuring dashboard reports" on page 1014.

### Using the date widget to schedule reports

The date widget specifies dates for reports.

The date widget enters the date for you. You can click **Today** to enter the current date.

### To use the date widget

- Click the date widget.
- Click the left arrow or the right arrow on either side of the month to change the
- Click the left arrow or the right arrow on either side of the year to change the
- Click the desired date on the calendar.

### Editing custom dashboards and reports

You can edit any custom report or dashboard that you create.

#### To edit a custom dashboard or report

In the Enforce Server administration console, on the Incidents menu, select Incident Reports.

The Incident Reports dashboard appears and displays Saved Reports near the top.

Click the edit icon next to the report or dashboard to edit.

The Save Report screen or the Save Dashboard screen appears. You can edit the name, description, and schedule of any custom report or dashboard, and you can select different component reports for a custom dashboard.

See "Saving custom incident reports" on page 1022.

3 When you finish editing, click Save.

## **Exporting incident reports**

A report can be exported to a comma-separated text (.csv) file or to an XML file.

You can set up a CSV delimiter other than a comma. You can specify which fields are exported to XML. These options must be set in your profile before you export a report.

See "Editing a user profile" on page 60.

#### To export a report

- 1 Click **Incidents**, and select a type of report.
- 2 Navigate to the report that you want to export. Filter or summarize the incidents in the report, as desired.
  - See "Common incident report features" on page 1039.
- Check the boxes on the left side of the incidents to select the incidents to export.
- 4 In the Export drop-down, select Export All: CSV or Export All: XML

Note: The XML schema files for exported reports are located in the C:\SymantecDLP\Protect\tomcat \lib\incidentapi-2011-schema.jar file.

See the Reporting API Developers Guide for a description of individual XML elements.

Click Open or Save. If you selected Save, a Save As dialog box opens, and you can specify the location and the file name.

See "Exported fields for Network Monitor" on page 1030.

See "Exported fields for Endpoint Discover" on page 1033.

See "Exported fields for Network Discover" on page 1031.

See "Exported fields for Mobile Prevent for Web" on page 1032.

See "Printing incident reports" on page 1042.

See "Sending incident reports by email" on page 1041.

## **Exported fields for Network Monitor**

The following fields are exported for Network Monitor:

Type Incident type (for example SMTP, HTTP, or FTP).

Message Status of this incident message.

**Status** 

Severity Severity of this incident (High, Medium, or Low).

Sent Date and time the message was sent.

ID Unique identifier for this incident. **Policy** Name of the policy that triggered this incident.

Matches The number of times that this item matches the detection parameters of a

policy rule.

Subject Subject of the message.

Recipient(s) Recipient of the message.

**Status** Status of this incident (New, Escalated, Dismissed, or Closed).

Has Indicates if this message has an attachment.

Attachment

**Data Owner** The person responsible for remediating the incident. This field must be set

Name manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

**Data Owner** The email address of the person responsible for remediating the incident.

**Email** This field must be set manually, or with one of the lookup plug-ins.

Custom attributes are also exported.

### **Exported fields for Network Discover**

The following fields are exported for Network Discover:

Type Target type (for example file system, Lotus Notes, or SQL Database).

Message

Status of this incident message.

**Status** 

Severity Severity of this incident (High, Medium, or Low).

Date that an incident was detected. Detection

Date

**Seen Before** Was this incident previously seen? The value is **Yes** or **No**.

Subject Email subject for integrated Exchange scans.

Sender Email sender for integrated Exchange scans.

Recipient Email recipient for integrated Exchange scans.

ID Unique identifier for this incident.

**Policy** Name of the policy that triggered this incident. Matches The number of times that this item matches the detection parameters of a

policy rule.

Location Location (path) of this item.

Status Status of this incident (New, Escalated, Dismissed, or Closed).

**Target** Name of the scan target.

Scan Date and time when the file was scanned.

File Owner Owner of the file.

Date and time when the item was last modified Last

Modified Date

File Create Date and time when the item was created

Date

Last Access Date and time when the item was last accessed.

Date

Name

Data Owner The person responsible for remediating the incident. This field must be set

manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

Data Owner The email address of the person responsible for remediating the incident. Email

This field must be set manually, or with one of the lookup plug-ins.

Custom attributes are also exported.

### **Exported fields for Mobile Prevent for Web**

The following fields are exported for Mobile Prevent for Web:

Incident type (for example HTTP/S or FTP). Type

Message **Status** 

Status of this incident message.

Severity Severity of this incident (High, Medium, or Low).

Sent Date and time the message was sent.

ID Unique identifier for this incident.

**Policy** Name of the policy that triggered this incident. Matches The number of times that this item matches the detection parameters of a

policy rule.

Subject Subject of the message.

Recipient(s) Recipient of the message.

**Status** Status of this incident (New, Escalated, Dismissed, or Closed).

Has Indicates if this message has an attachment.

Attachment

**Data Owner** The person responsible for remediating the incident. This field must be set

Name manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

**Data Owner** The email address of the person responsible for remediating the incident.

**Email** This field must be set manually, or with one of the lookup plug-ins.

### **Exported fields for Endpoint Discover**

The following fields are exported for Endpoint Discover:

Target type (for example Removable Storage). Type

Severity Severity of this incident (High, Medium, or Low).

Occurred On Date that an incident was detected.

ID Unique identifier for this incident.

**Policy** Name of the policy that triggered this incident.

Matches The number of times that this item matches the detection parameters of a

policy rule.

**Status** Status of this incident (New, Escalated, Dismissed, or Closed).

File Name Name of the file that violated the policy.

File Path Path of the file

**Note:** The file location appears only for fixed drive incidents.

Machine Computer on which the incident occurred.

User Endpoint user name. Prevention Status from Endpoint (for example Action Blocked).

**Status** 

Subject Subject of the message.

Recipient(s) Recipient of the message.

Has Indicates if this message has an attachment.

Attachment

**Data Owner** The person responsible for remediating the incident. This field must be set

Name manually, or with one of the lookup plug-ins.

Reports can automatically be sent to the data owner for remediation.

**Data Owner** The email address of the person responsible for remediating the incident. Email

This field must be set manually, or with one of the lookup plug-ins.

Custom attributes are also exported.

# **Deleting incidents**

Incident reporting performance often deteriorates when the number of incidents in your system exceeds one million (1,000,000). Symantec recommends keeping your incident count below this threshold by deleting incidents to maintain good system performance.

Incident deletion is permanent: you can delete incidents, but you cannot recover the incidents that you have deleted. Symantec Data Loss Prevention offers options for deleting only certain parts of the data that triggered the incident.

After you have marked incidents for deletion, you can view, configure, run, and troubleshoot the incident deletion process from the Enforce Server administration console.

For information about deleting archived incidents, See "Deleting archived incidents" on page 1068.

### To delete an incident

- On the Incident Report screen, select the incident or incidents you want to delete, then click Incident Actions > Delete Incidents.
- 2 On the **Delete Incidents** screen, select from the following deletion options:

Delete incident completely

Permanently deletes the incident(s) and all associated data (for example, any emails and attachments). Note that you cannot

recover the incidents that have been deleted

Retain incident, but delete message data

Retains the actual incident(s) but discards the Symantec Data Loss Prevention copy of the data that triggered the incident(s). You have the option of deleting only certain parts of the associated data. The rest of the data is preserved.

### **Delete Original** Message

Deletes the message content (for example, the email message or HTML post). This option applies only to Network incidents.

# Delete

This option refers to files (for Endpoint and Discover incidents) or Attachments/Files email or posting attachments (for Network incidents). The options are:

- All, which deletes all attachments. Choose this option to delete all files (for Endpoint and Discover incidents) or email attachments (for Network incidents). Attachments and files are added to the incident deletion queue after their associated incidents have been deleted.
- Attachments/Files with no violations. This option deletes only those attachments in which Symantec Data Loss Prevention found no matches. Choose this option when you have incidents with individual files taken from a compressed file (Endpoint and Discover incidents) or several email attachments (Network incidents).

#### 3 Click Cancel or Delete.

**Delete** marks the incident for deletion and adds it to the incident deletion queue. You cannot recover an incident after it has been marked for deletion. Symantec Data Loss Prevention permanently deletes the incidents in the incident deletion queue when it runs the incident deletion job.

### About the incident deletion process

You can view, configure, run, and troubleshoot the incident deletion process on the Incident Deletion screen of the Enforce Server administration console: System > Incident Data > Incident Deletion. This screen shows you the number of incidents in the incident deletion queue, the deletion schedule, and a history of deletion jobs.

The incident deletion queue includes all incidents marked for deletion by all your Symantec Data Loss Prevention users. In addition to viewing the number of incidents marked for deletion, you can start and stop a deletion job manually from the incident deletion queue.

You can view detailed information about your deletion jobs in the deletion jobs history section, including the number of incidents and attachments or files deleted, the job start and end time, the job duration, whether or not the job was stopped

manually, and the job status (Completed, Failed, or In Progress). In the case of failed deletion jobs, you can click the Failed link to see the error message and problem statement. This information may be useful to your Oracle database administrator in troubleshooting the job failure. If this information is insufficient to resolve your deletion job issues, you can export information from any job to a CSV file and send it to Symantec Data Loss Prevention Support for additional help.

By default, the incident deletion job runs nightly at 11:59 P.M. in the Enforce Server's local time zone. When the job runs, it also creates an event on the System > Server > Events screen. This event is created whether or not any incidents are actually deleted.

### Configuring the incident deletion job schedule

The default incident deletion job schedule is daily at 11:59 P.M. in the Enforce Server's local time zone. You can configure the deletion job schedule to run at any other scheduled time. Symantec suggests running your incident deletion at a time when your system is idle or not in heavy use.

### To configure the incident deletion job schedule

- 1 Click the **Schedule Deletion Job** calendar icon.
- 2 In the Schedule Incident Deletion dialog box, specify one of the following options:
  - No Regular Schedule: Select this option to turn off the deletion job schedule.
  - Once: Specify a day and time for a single incident deletion job.
  - **Daily**: Specify a daily time for incident deletion jobs.
  - **Weekly**: Specify a day and time for incident deletion jobs.
  - **Monthly**: Specify a day of the month and time for incident deletion jobs. To accommodate differences between months, the day value must be between 1 and 28.

#### 3 Click Submit.

Note: The incident deletion job schedule is reset to the default value during the upgrade process. If you are using a custom incident deletion job schedule, reconfigure the schedule after the upgrade process is complete.

### Starting and stopping incident deletion jobs

If there are incidents pending deletion, you can start an incident deletion job manually from the incident deletion queue. You can also stop any incident deletion job that is currently running.

### To start and stop incident deletions job manually

- Click **Start Deletion** to start an incident deletion job manually.
- When an incident deletion job is running, the progress bar will show you how many incidents have been deleted.
- 3 Click **Stop Deletion** to stop an incident deletion job.

The progress bar refreshes every 30 seconds by default. If you are deleting a large number of incidents (over 500,000), the refresh process may degrade the performance of the deletion job. You can adjust the refresh rate in the manager.properties file.

#### To configure the progress bar refresh rate

- Open the manager.properties file:
  - On Windows systems: \SymantecDLP\Protect\config\manager.properties
  - On Linux systems: /opt/SymantecDLP/Protect/config/manager.properties
- 2 Set a new value in milliseconds for the

com.vontu.incident.deletion.progress.refreshRate property. For example, to set the refresh rate to two minutes (120 seconds):

```
com.vontu.incident.deletion.progress.refreshRate=120000
```

3 Save and close the manager.properties file, then restart the Vontu Manager service.

See "About Data Lost Prevention services" on page 76.

### Working with the deletion jobs history

The deletion jobs history section shows you your previously run incident deletion jobs, including:

- The number of incidents deleted.
- The number of attachments and files deleted.
- The deletion job start and end time.

- The deletion job duration.
- Whether or not the deletion job was stopped manually.
- The deletion job status.

If a deletion job failed, a link will appear in the status column. Click the link to see the error message and problem statement. This information may be useful to your Oracle database administrator for troubleshooting a failed deletion job.

If you are having trouble troubleshooting incident deletion job issues, you can export detailed deletion job information to send to Symantec Data Loss Prevention Support.

### To view and export failed deletion job information

- In the **Deletion jobs history** list, click the **Failed** link for the failed job you want to view.
  - The error message and problem statement that appear may be useful to your Oracle database administrator for troubleshooting your incident deletion job issues. If you need additional help, continue to step 2.
- 2 To export information for a failed deletion job, select the job in the **Deletion** jobs history list, then click Export.
- 3 Save the ZIP file to send to Symantec Data Loss Prevention Support for analysis. The data contained in the ZIP file is intended for use by Symantec Data Loss Prevention Support only, and will not be helpful for your in-house troubleshooting efforts.

## Deleting custom dashboards and reports

You can delete any custom report or dashboard that you create.

#### To delete a custom dashboard or report

- In the Enforce Server administration console, on the **Incidents** menu, select Incident Reports.
  - The Incident Reports dashboard appears and displays Saved Reports near the top.
- Click the delete icon next to the report or dashboard to delete it.
- 3 Click **OK** to confirm.
- Symantec Data Loss Prevention deletes the report, and removes it from the Incident Reports screen.

### Common incident report features

The following options are common to incident report lists:

Icons to perform the following tasks for a report:

#### Save

You can save the current report as a custom saved report. See "Saving custom incident reports" on page 1022.

#### Send

You can email the report or schedule the report distribution. See "Saving custom incident reports" on page 1022.

### Export

You can export the current report as CSV or XML. See "Exporting incident reports" on page 1029.

#### Delete Report

If this report is not a saved report, then the Delete Report option does not appear.

 Report filters and summary options See "Incident report filter and summary options" on page 1040.

 Page navigation icons See "Page navigation in incident reports" on page 1039.

The following summary reports are available for the types of incidents:

Network See "Network summary report" on page 961.

Endpoint

See "Endpoint incident summary reports" on page 975.

Discover

See "Discover summary reports" on page 999.

Mobile

See "Mobile summary report" on page 986.

## Page navigation in incident reports

All reports except executive summaries include page navigation options. Symantec Data Loss Prevention displays the number of currently visible incidents out of total report incidents (for example, 1-19 of 19 or 1-50 of 315).

Reports with more than 50 incidents have the following options:

Displays the first page of the report.

Displays the previous page.

Displays the next page.

bb Displays the last page.

Show All Displays all items on one single page.

> Use the **Show All** link on an **Incident List** with caution when the system contains more than 500 incidents. Browser performance degrades drastically if more than 500 incidents are displayed on the **Incident List**

page.

Select All Selects all incidents on all pages, so you can update them all at once.

(Available only on Incident Lists.) Click Unselect All to cancel.

Note: Use caution when you choose Select All. This option selects all the incidents in the report (not only those on the current page). Any incident command that you subsequently apply affects all the incidents.

To select only the incidents on the current page, select the checkbox

at top left of the incident list.

See "Common incident report features" on page 1039.

# Incident report filter and summary options

Filters are separated into commonly used filters, and advanced filters and summarizations.

The common filters include the following options:

Status Select Equals, Is Any Of, or Is None Of. Then select status

> values. Hold down Ctrl and click to select more than one separate status value. Hold down Shift and click to select a

range.

Date Use the drop-down menu to select a date range, such as

Last Week or Last Month. The default is All Dates. Network and Endpoint reports

Severity Check the boxes to select the severity values.

Scan For Discover reports, select the scan to report. You can select

the most recent scan, the initial scan, or a scan in progress. Discover reports

All Scans is the default.

**Target ID** 

For Discover reports, select the name of the target to report. All Targets is the default.

Click the Advanced Filters & Summarization bar to expand the section with filter and summary options.

Click Add Filter to add an advanced filter.

Select a primary and optional secondary option for summarization. A single-summary report is organized with a single summary criterion, such as the policy that is associated with each incident. A double-summary report is organized with two criteria, such as policy and incident status.

Note: If you select a condition in which you enter the content to be matched in the text field, your entire entry must match exactly. For example, if you enter "apples and oranges", that exact text must appear in the specified component for it to be considered a match. The sentence "Bring me the apples and the oranges" is not considered a match.

For a complete list of the report filter and summary options, see the Symantec Data Loss Prevention Administration Guide.

See "Common incident report features" on page 1039.

## Sending incident reports by email

You can send a copy of the current report to any email address.

To send reports, your system administrator must configure an SMTP server. The Administrator must specify a report distribution option on the **System > Settings** page. You must also specify an email address for your user account.

See "Configuring the Enforce Server to send email alerts" on page 146.

### To send a report

- Click **Incidents**, and select a type of report.
- Navigate to the report that you want to export. Filter or summarize the incidents in the report, as desired.
  - See "Common incident report features" on page 1039.
- 3 Click **Send** in the upper right corner.
  - Alternatively, you can use the **Send** menu (above the filters).
  - See "Saving custom incident reports" on page 1022.

In the **Send Report** dialog box, specify the following options:

To Enter one or more email addresses (comma-separated).

Subject Enter a subject for the message.

Message Enter the message.

5 Click Send or Cancel.

See "Printing incident reports" on page 1042.

See "Exporting incident reports" on page 1029.

### **Printing incident reports**

You can print a report to any available printer.

### To print a report

- 1 Click Incidents, and select a type of report.
- 2 Navigate to the report that you want to export. Filter or summarize the incidents in the report, as desired.

See "Common incident report features" on page 1039.

- 3 Click **Print** in the upper right corner.
- 4 An image of the report appears in a browser window.
- 5 The printer selection dialog box appears, and you can select a printer.

See "Sending incident reports by email" on page 1041.

See "Exporting incident reports" on page 1029.

## Incident snapshot history tab

You can view the actions that were performed on the incident. For each action, the History tab displays the action date and time, the actor (a user or server), and the action or the comment. Click Add Comment to add a comment.

See "Discover incident snapshots" on page 991.

See "Network incident snapshot" on page 956.

See "Endpoint incident snapshot" on page 967.

See "Mobile incident snapshot" on page 978.

### Incident snapshot attributes section

You can view a list of custom attributes and their values, if any have been specified. Click on attribute values to view an incident list that is filtered on that value. To add new values or edit existing ones, click Edit. In the Edit Attributes dialog box that appears, type the new values and click Save. Archived incidents are not displayed in the filtered list.

Note: This section appears only if a system administrator has configured custom attributes.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Network incident snapshot" on page 956.

See "Mobile incident snapshot" on page 978.

### Incident snapshot correlations tab

You can view lists of the incidents that share various attributes of the current incident.

For example, if the copying of a file triggered the current incident, you can bring up a list of all the incidents that are related to the copying of this file. The Correlations tab shows a list of correlations that are matched to single attributes. Click on attribute values to view lists of the incidents that are related to those values.

To search for other incidents with the same attributes, click **Find Similar**. In the Find Similar Incidents dialog box that appears, select the desired search attributes. Then click **Find Incidents**. Archived incidents are not displayed when you search for similar incidents.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Network incident snapshot" on page 956.

See "Mobile incident snapshot" on page 978.

## Incident snapshot policy section

The Policy area shows the policy that was violated in the incident and indicates if the policy blocked a move or notified the user. It also shows the total number of matches for the policy, as well as matches per policy rule. Click the policy name to view a list of all incidents that violated the policy. Click view policy to view a read-only version of the policy.

You see the icons that describe the following information:

- Symantec Data Loss Prevention blocked a copy of the sensitive information.
- Symantec Data Loss Prevention notified the user about the copy of confidential data.

This section also lists other policies that are violated from the same file. To view the snapshot of an incident that is associated with a particular policy, click the Go to Incident link next to the policy name. To view a list of all incidents that are related to the file, click show all.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Network incident snapshot" on page 956.

See "Mobile incident snapshot" on page 978.

# Incident snapshot matches section

In the Matches section, Symantec Data Loss Prevention displays the content (if applicable) and the matches that caused the incident.

Matches are highlighted in yellow. This section shows the match total and displays the matches in the order in which they appear in the original content. To view the rule that triggered a match, click on the highlighted match.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Network incident snapshot" on page 956.

See "Mobile incident snapshot" on page 978.

See "About the Similarity Threshold and Similarity Score" on page 512.

## Incident snapshot access information section

The Access Information section of an incident snapshot shows the Access Control Lists for that object.

Access Control Lists (ACL) are lists of the permissions that are attached to an object or piece of data. The list contains information about all users who have read and write permissions for the file. Use the list to view which users have access to the file as well as which actions each user can perform. The permissions for each user or group are not set through Symantec Data Loss Prevention. Administrators set the permissions for each file using other types of programs on the endpoint. Permissions are generally set at the time that the file is created.

For example, User 1 has permission to access the file Example 1. doc. User 1 can view and edit the file. User 2 also has access to the file Example1.doc. However, User 2 can only view the file. User 2 does not have permission to make changes to the file. In the ACL, both User 1 and User 2 are listed with the permissions that have been granted to them.

Table 46-1 shows the combinations.

Table 46-1 Access control list example

Name	Permission
User 1	GRANT READ
User 1	GRANT WRITE
User 2	GRANT READ

The ACL contains a new line for each permission granted. The ACL only contains one line for User 2 because User 2 only has one permission, to read the file. User 2 cannot make any changes to the file. User 1 has two entries because User 1 has two permissions: reading the file and editing it.

You can view ACL information only on Discover and Endpoint local drive incident snapshots. You cannot view ACL information on any other type of incidents.

The Access Information section appears on the Key Info tab of the incident snapshot.

See "Discover incident snapshots" on page 991.

See "Endpoint incident snapshot" on page 967.

See "Network incident snapshot" on page 956.

See "Mobile incident snapshot" on page 978.

## **Customizing incident snapshot pages**

You can customize the appearance of the incident snapshot page.

#### To customize the appearance of the incident snapshot page

- 1 From an incident snapshot, click **Customize Layout** (in the upper-right corner).
- 2 Select the information to appear on each of the tabs in the incident snapshots. Tab 1 always contains the **Key Info**, and cannot be changed.
- 3 For each of the areas on the incident snapshot screen, select the information that appears.
- Click Save.

## About filters and summary options for reports

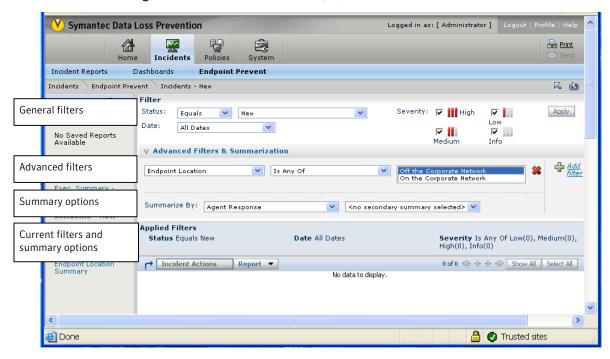
You can set a number of filters and summaries for Symantec Data Loss Prevention incident reports.

These filters let you see the incidents and incident data in different ways.

The set of filters apply separately to Network, Endpoint, Mobile, and Storage events.

Figure 46-1 shows the locations of the options to filter and summarize reports.

Figure 46-1 Filter and summary options



The filters and summary options are in the following sections:

General filters The general filter options are See "General filters for

> the most commonly used. reports" on page 1047.

They are always visible in the

incident list report.

Advanced filters The advanced filters provide See "Advanced filter options

many additional filter options. for reports" on page 1056.

You must click the Advanced Filters & Summarization bar, and then click Add Filter to view these filter options.

Summary options The summary options provide See "Summary options for

ways to summarize the

incident reports" on page 1051.

incidents in the list. You must click the Advanced Filters & Summarization bar to view these summary options.

Symantec Data Loss Prevention contains many standard reports. You can also create custom reports or save report summary and filter options for reuse.

See "About Symantec Data Loss Prevention reports" on page 1006.

## General filters for reports

General filters for reports include a set of a few common filters.

Most of these filters are applicable for all the products. Network Discover contains some general filters that relate to scans of storage. For example, you can filter the incidents that are in a particular scan. These filters are not applicable to Network Prevent or Endpoint Prevent.

Table 46-2 lists the general filter options for report status values.

You can also create custom status values.

See "About incident status attributes" on page 1069.

These status filters are available for Network, Endpoint, Mobile, and Discover incidents.

Table 46-2 General filters for status values

Name	Description
Equals	The status is equal to the field that is selected in the next drop-down.
Is Any Of	The status can be any of the fields that are selected in the next drop-down. Shift-click to select multiple fields.
Is None Of	The status is none of the fields that are selected in the next drop-down. Shift-click to select multiple fields.

Table 46-3 lists the general filter options by date.

These date filters are available for Network, Mobile, and Endpoint incidents.

General filters by date **Table 46-3** 

Name	Description
All Dates	All of the dates that contain incidents.
<b>Current Month to Date</b>	All of the incidents that were reported for the current month up to today's date.
Current Quarter to Date	All of the incidents that were reported for the current quarter up to today's date.
<b>Current Week to Date</b>	All of the incidents that were reported for the current week.
Current Year to Date	All of the incidents that have been reported for the current year up to today's date.
Custom	A custom time frame. Select the dates that you want to view from the calendar menu.
Last 7 Days	All of the incidents that were reported in the previous seven days.
Last 30 Days	All of the incidents that were reported in the previous 30 days.
Last Month	All of the incidents that were reported during the previous calendar month.
Last Week	All of the incidents that were reported during the previous calendar week.
Last Quarter	All of the incidents that were reported during the previous quarter.
Last Year	All of the incidents that were reported during the last calendar year.

Table 46-3 General filters by date (continued)

Name	Description
Today	All of the incidents that were reported today.
Yesterday	All of the incidents that were reported yesterday.

Table 46-4 lists the general filter options by severity. Check the box to select the severities to include in the filter.

These severity filters are available for Network, Endpoint, Mobile, and Discover incidents.

**Table 46-4** General filters for severity values

Name	Description
High	Lists only the high-severity incidents. Displays how many high-severity incidents are in the incident list.
Info	Lists only the incidents that are informational only. Informational incidents are not assigned any other severity. Displays how many informational incidents are in the incident list.
Low	Lists only the low-severity incidents. Displays how many low-severity incidents are in the incident list.
Medium	Lists only the medium-severity incidents. Displays how many medium-severity incidents are in the incident list.

Table 46-5 lists the general filter options for Network Discover scans. This filter is only available for Discover incidents.

General filters for scans **Table 46-5** 

Name	Description
All Scans	All of the incidents that have been reported in all of the scans that have been run.
Initial Scan	All of the incidents that were reported in the initial scan.
In Process	All of the incidents that have been reported in the scans that are currently in progress.
Last Completed Scan	All of the incidents that were reported in the last complete scan.

You can filter Discover incidents by Target ID. This filter is only available for Discover incidents.

Select the target, or select **All Targets**. Shift-click to select multiple fields.

Table 46-6 lists the general filter options by detection date for Discover incidents.

General filters by date **Table 46-6** 

Name	Description
All Dates	All of the dates that contain incidents.
<b>Current Month to Date</b>	All of the incidents that were reported for the current month up to today's date.
Current Quarter to Date	All of the incidents that were reported for the current quarter up to today's date.
<b>Current Week to Date</b>	All of the incidents that were reported for the current week.
Current Year to Date	All of the incidents that have been reported for the current year up to today's date.
Custom	A custom time frame. Select the dates that you want to view from the calendar menu.
Custom Since	The Symantec DLP Agents that have connected to the Endpoint Server from a specific date to the present date. Select the date where you want the filter to begin.
Custom Before	The Symantec DLP Agents that have connected to an Endpoint Server before a specific date. Select the final date for the filter.
Last 7 Days	All of the incidents that were reported in the previous seven days.
Last 30 Days	All of the incidents that were reported in the previous 30 days.
Last Month	All of the incidents that were reported during the previous calendar month.
Last Week	All of the incidents that were reported during the previous calendar week.
Last Quarter	All of the incidents that were reported during the previous quarter.
Last Year	All of the incidents that were reported during the last calendar year.
Today	All of the incidents that were reported today.
Yesterday	All of the incidents that were reported yesterday.

## Summary options for incident reports

Incident report summaries provide options for a summary of the information that is contained within the incidents. For example, you can summarize incidents by the status or the policy.

Note: Archived incidents are not included in report summaries unless the Advanced filter option for the Is Archived filter is set to Show Archived and non-Archived incidents.

See "About incident archiving" on page 1065.

Table 46-7 lists the summary options for incident reports.

**Table 46-7** Summary filters

Name	Description	Applicable products
Agent Configuration	Summarize the agents and incidents by the associated agent configuration entity. If you have more than one agent configuration entity configured, you can summarize or filter by a specific entity drop down menu. If the default agent configuration entity is the only entity configured, you will not see the drop down menu.	Endpoint
Agent Response	Summarize incidents by how the agent has responded to the incident.	Endpoint
Content Root	Summarize the incidents by the content root path.	Discover
Data Owner Email Address	The email address of the person responsible for remediating the incident. This field must be set manually, or with a lookup plug-in.	Network Endpoint Discover

Summary filters (continued) **Table 46-7** 

Name	Description	Applicable products
Data Owner Name	The person responsible for remediating the incident. This field must be set manually, or with a lookup plug-in.  Reports can automatically be sent to the data owner for remediation.	Network Endpoint Discover Mobile
Destination IP	Summarize the incidents by the destination IP address.	Network Endpoint
<b>Detection Month</b>	Summarize the incidents by the month in which they were detected.	Discover
Detection Quarter	Summarize the incidents by the calendar quarter in which they were detected.	Discover
Detection Week	Summarize the incidents by the week in which they were detected.	Discover
Detection Year	Summarize the incidents by the year in which they were detected.	Discover
Device Instance ID	Summarize the incidents by the specific device that created the violation.	Endpoint
Domain	Summarize the incidents by the domain name.	Network
Email	Summarize the incidents by the email associated with the violation.	Mobile
Endpoint Location	Summarize the incidents by the location of the endpoint.  The location can be one of the following:  On the Corporate Network  Off the Corporate Network	Endpoint
File Name	Summarize the incidents by the file name that is associated with the incident.	Endpoint

Summary filters (continued) Table 46-7

Name	Description	Applicable products
File Owner	Summarize the incidents by the owner of the file.	Discover
Investigating State	Summarize the agents by the current status.	Endpoint Discover
Location	Summarize the incidents by their location.	Discover
Log Level	Summarize the agents by their configured log levels.	Endpoint
Machine IP (Corporate)	Summarize the incidents by the IP address of a machine on the corporate network.	Endpoint
Machine Name	Summarize the incident by the computer name on which the incidents were created.	Endpoint
Month	Summarize the incidents by the month in which they were created.	Network Endpoint Mobile
Months Since First Detected	Summarize the incidents by how many months have passed since the incident was first detected.	Discover
Network Prevention Action	Summarize the incidents by the action from Network Prevent.	Network
No primary summary selected	Placeholder selection to denote that no primary summary has been selected.	Network Endpoint Discover
No secondary summary selected	Placeholder selection to denote that no summary has been selected.	Network Endpoint Discover

Summary filters (continued) **Table 46-7** 

Name	Description	Applicable products
Policy	Summarize the incidents by the policy from which they were created.	Network Endpoint Discover Mobile
Policy Group	Summarize the incidents by the policy group to which they belong.	Network Discover Mobile
Policy rule	Summarize the incidents by the policy rule which generated the violation.	Mobile
Protect Status	Summarize the incidents by the Network status of the incidents.	Discover
Protocol	Summarize the incidents by the protocol that generated the incident.	Network Mobile
Protocol or Endpoint Destination	Summarize the incidents by the protocol or the endpoint destination where the incidents were created.	Endpoint
Remediation Detection Status	Summarize the incidents by their remediation detection status.	Discover
Quarantine Failure Reason	Summarize the incidents by the reason that the quarantine response action failed.	Endpoint Discover
Quarter	Summarize the incidents by the quarter in which they were created.	Network Endpoint Mobile
Quarters Since First Detected	Summarize the incidents by how many quarters have passed since the incident was first detected.	Discover
Recipient	Summarize the incidents by the recipient.	Discover

Summary filters (continued) **Table 46-7** 

Name	Description	Applicable products
Scan	Summarize the incidents by which scan was used to find the incidents.	Discover
Scanned Machine	Summarize the incidents by the computers that have been scanned.	Discover
Sender	Summarize the incidents by the sender.	Network Endpoint Discover
Server	Summarize the incidents by the server on which they were created.	Network Endpoint Mobile
Source IP	Summarize the incidents by the source IP address from which they were created.	Network Endpoint Mobile
Source File	Summarize the incidents by the source file that violated the policy.	Endpoint
Status	Summarize the incidents by the incident status.	Network Endpoint Discover Mobile
Subject	Summarize the incidents by the subject.	Discover
Mobile Prevent Action	Summarize the incidents by the response rule action that was taken.	Mobile
Target ID	Summarize the incidents by the target scan ID.	Discover
Target Type	Summarize the incidents by the type of target on which the incident was generated.	Discover
User Justification	Summarize the incidents by the justification that was input by the user.	Endpoint

	, ,	
Name	Description	Applicable products
User Name	Summarize the incidents by the user who generated the incident.	Endpoint
Week	Summarize the incidents by the week in which they were created.	Network Endpoint Mobile
Weeks Since First Detected	Summarize the incidents by how many weeks have passed since the incident was first detected.	Discover
Year	Summarize the incidents by the year in which they were created.	Network Endpoint Mobile
Years Since First Detected	Summarize the incident by how many years have passed since the incident was first detected.	Discover

**Table 46-7** Summary filters (continued)

## Advanced filter options for reports

Advanced report filters let you filter incidents related to specific actions or text strings. For example, you can filter the incidents that relate to a specific keyword. Or, you can filter out the incidents that relate to a certain action. These filters combine a set of chooser fields or text boxes to create the advanced filter.

Table 46-8, Table 46-9, and Table 46-10 list the advanced filter options for reports.

**Table 46-8** Advanced filters, first field

Name	Description	Applicable products
Agent Configuration	Summarize the agents and incidents by the associated agent configuration entity. If you have more than one agent configuration entity configured, you can summarize or filter by a specific entity drop down menu. If the default agent configuration entity is the only entity configured, you will not see the drop down menu.	Endpoint

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
Agent Configuration Status	Summarize the agent by the status of the configuration entity.	Endpoint
	<ul> <li>Current Configuration         The configuration on the agent is the same as the configuration on the Endpoint Server.     </li> <li>Outdated Configuration         The configuration on the agent is different than the configuration on the Endpoint Server.     </li> <li>Unknown/deleted Configuration         The agents either cannot report which configuration is installed, or the configuration on the agent has been deleted from the Endpoint Server.     </li> </ul>	
Agent Response	Filter incidents by how the agent has responded to the incident.	Endpoint
Application Name	Filter the incidents by the name of the application where the incident was generated.	Endpoint
Application Window Title	Filter the incidents by a string in the title of the window where the incident was generated.	Endpoint
Attachment File Name	Filter incidents by the file name of the attachment that is associated with the incident.	Network Mobile
Attachment File Size	Filter incidents by the size of the attachment that is associated with the incident.	Network Mobile
Content Root	Filter the incidents by the content root path.	Discover
Data Owner Email Address	The email address of the person responsible for remediating the incident. This field must be set manually, or with a lookup plug-in.	Network Endpoint Discover Mobile

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable
		products
Data Owner Name	The person responsible for remediating the incident. This field must be set manually, or with	Network
	a lookup plug-in.	Endpoint
	Reports can automatically be sent to the data	Discover
	owner for remediation.	Mobile
Destination IP	Filter the incidents by the destination IP address	Network
	for the message that generated the incident.	Endpoint
		Mobile
Detection Date	Filter the incidents by the date that the incident was detected.	Discover
Device Instance ID	Summarize the incidents by the specific device that created the violation.	Endpoint
Document Name	Filter the incidents by the name of the violating document.	Discover
Domain	Filter the incidents by the domain name that is associated with the incident.	Network
Email	Filter the incidents by the email address to which they are associated.	Mobile
Endpoint Location	Filter the incidents by the endpoint location.	Endpoint
	The location can be one of the following:	
	<ul><li>On the Corporate Network</li><li>Off the Corporate Network</li></ul>	
File Last Modified Date	Filter the incidents by the last date when the file	Endpoint
	was modified.	Discover
File Location	Filter the incidents by the location of the violating file.	Endpoint
File Name	Filter the incidents by the name of the violating	Endpoint
	file. No wildcards, but you can specify a partial match, for example .pdf.	Discover

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
File Owner	Filter the incidents by the owner of the violating files.	Discover
File Size	Filter the incidents by the size of the violating file.	Endpoint Discover
Incident History Issuer	Filter the incidents by the user responsible for issuing the history of the incident.	Network Endpoint Discover Mobile
Incident ID	Filter the incidents by the ID of the incidents.	Network Endpoint Discover Mobile
Incident Match Count	Filter the incidents by the number of incident matches.	Network Endpoint Discover Mobile
Incident Notes	Filter the incidents by a string in the incident notes.	Network Endpoint Discover Mobile
Incident Reported On	Filter the incidents by the date that the incident was reported.	Endpoint
Investigating State	Filter the agents by the investigation state. You can select one of the following:  Investigating  Not Investigating	Discover Endpoint

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
Is Archived	Filters archived incidents. You can select one of the following:  Show Archived and non-Archived Incidents Show Archived  See "About incident archiving" on page 1065.	Network Endpoint Discover Mobile Classification
Is Archive Allowed	Filters the incidents based on the state of the Is Archived Allowed flag. Select the Is Any Of operator from the second field, then select either the Allow Archive or Do Not Archive option from the third field.  See "About incident archiving" on page 1065.	Network Endpoint Discover Mobile Classification
Last Connection Time	Filter agents according to the last time each agent connected to the Endpoint Server.	Endpoint
Location	Filter the incidents by their location. Location can include the server where the incidents were generated.	Discover
Machine IP (Corporate)	Filter the incidents by the IP address of the computer on which the incidents were created.	Endpoint
Machine Name	Filter the incidents by the computer name on which the incidents were created.	Endpoint
Minimum Similarity Score	Filter the incidents by how similar the violations are to each other.	Mobile
Network Prevent Action	Filter the incidents by the action from Network Prevent.	Network
Policy	Filter the incidents by the policy from which they were created.	Network Endpoint Discover Mobile

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
Policy Group	Filter the incidents by the policy group to which they belong.	Network Endpoint Discover Mobile
Policy Rule	Filter the incidents by the policy rule that generated the incidents.	Network Endpoint Discover Mobile
Protect Status	Filter the incidents by the Network Protect status of the incidents.	Discover
Protocol	Filter the incidents by the protocol to which they belong.	Network Mobile
Protocol or Endpoint Destination	Filter the incidents by the protocol or the endpoint destination that generated the incident.	Endpoint
Read ACL: File	Filter the incidents by the File access control list.	Endpoint Discover
Read ACL: Share	Filter the incidents by the Share access control list.	Discover
Recipient	Filter the incidents by the name of the recipient of the message that generated the incident.	Network Endpoint Discover
Remediation Detection Status	Filter the incidents by their remediation detection status.	Discover
Scanned Machine	Filter the incidents by the computers that have been scanned.	Discover
Seen Before	Filter the incidents on whether an earlier connected incident exists.	Discover, but not for SQL Database incidents (where Seen Before is always false)

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
Sender	Filter the incidents by the sender.	Network
		Endpoint
		Discover
Server	Filter the incidents by the server on which they	Network
	were created.	Endpoint
		Discover
		Mobile
SharePoint ACL: Permission Level	Filter the incidents on the permission level of the SharePoint access control list.	Discover
SharePoint ACL: User/Group	Filter the incidents on the user or group in the SharePoint access control list.	Discover
Source IP	Filter the incidents by the source IP address	Network
	from which they were created.	Mobile
Subject	Filter incidents by the subject line of the	Network
	message that generated the incident.	Discover
Superseded	Filter the incidents by the incident responses	Discover
	have been superseded by other responses.	Endpoint
Mobile Prevent Action	Filter the incidents by the response rule action that was taken.	Mobile
Target Type	Filter the incidents by the type of target that is associated with the incidents.	Discover
Time Since First Detected	Filter the incidents by how much time has passed since the incident was first detected.	Discover, but not for SQL Database incidents
URL	Filter the incidents by the URL where the violations occurred.	Discover
User Justification	Filter the incidents by the justification that was input by the user.	Endpoint

Advanced filters, first field (continued) **Table 46-8** 

Name	Description	Applicable products
User Name	Filter the incidents by the user who generated the incident.	Endpoint

The second field in the advanced filters lets you select the match type in the filter.

**Table 46-9** Advanced filters, second field

Name	Description
Contains Any Of	Lets you modify the filter to include any words in the text string, or lets you choose from a list in the third field.
Contains Ignore Case	Lets you modify the filter to ignore a specific text string.
Does Not Contain Ignore Case	Lets you modify the filter to filter out the ignored text string.
Does Not Match Exactly	Lets you modify the filter to match on any combination of the text string.
Ends with Ignore Case	Lets you modify the filter so that only the incidents that end with the ignored text string appear.
Is Any Of	Lets you modify the filter so that the results include any of the text string, or lets you choose from a list in the third field.
Is Between	Lets you modify the filter so that the numerical results are between a range of specified numbers.
Is Greater Than	Lets you modify the filter so that the numerical results are greater than a specified number.
Is Less Than	Lets you modify the filter so that the numerical results are less than a specified number.
Is None Of	Lets you modify the filter so that the results do not include any of the text string, or lets you choose from a list in the third field.
Is Unassigned	Lets you modify the filter to match incidents for which the value specified in the first field are unassigned.
Matches Exactly	Lets you modify the filter to match exactly the text string.
Matches Exactly Ignore Case	Lets you modify the filter so that the filter must match the ignored text string exactly.

**Table 46-9** Advanced filters, second field (continued)

Name	Description
Starts with Ignore Case	Lets you modify the filter so that only the incidents that start with the ignored text string appear.

The third field in the advanced filters lets you select from a list of items, or provides an empty box to enter a string.

This third field varies depending on the selections in the first and second fields.

For a list of items, use Shift-click to select multiple items.

For strings, wildcards are not allowed, but you can enter a partial string.

For example, you can enter  $\mbox{.pdf}$  to select any PDF file.

If you do not know what text to enter, use the summary options to view the list of possible text values. You can also see a summary of how many incidents are in each category.

See "Summary options for incident reports" on page 1051.

Table 46-10 lists some of the options in the third field.

Table 46-10 Advanced filters, third field

Name	Description
Blocked	The user was blocked from performing the action that cause the incident.
Content Removed	The content in violation was removed.
No Remediation	No incident remediation has occurred for this incident.
None	No action was taken regarding the violation that caused the incident.
Protect File Copied	The file in violation was copied to another location.
Protect File Quarantined	The file in violation was quarantined to another location.
User Notified	The user was notified that a violation had occurred.

# Archiving incidents

This chapter includes the following topics:

- About incident archiving
- Archiving incidents
- Restoring archived incidents
- Preventing incidents from being archived
- Deleting archived incidents

## About incident archiving

Incident archiving lets you flag specified incidents as "archived." Because these archived incidents are excluded from normal incident reporting, you can improve the reporting performance of your Symantec Data Loss Prevention deployment by archiving any incidents that are no longer relevant. The archived incidents remain in the database; they are not moved to another table, database, or other type of offline storage.

You can set filters on incident reports in the Enforce Server administration console to display only archived incidents or to display both archived and non-archived incidents. Using these reports, you can flag one or more incidents as archived by using the **Archive** options that are available when you select one or more incidents and click the **Incident Actions** button. The **Archive** options are:

- Archive Incidents—Flags the selected incidents as archived.
- **Restore Incidents**—Restores the selected incidents to the non-archived state.
- **Do Not Archive**—Prevents the selected incidents from being archived.
- Allow Archive—Allows the selected incidents to be archived.

The archive state of an incident displays in the incident snapshot screen in the Enforce Server administration console. The **History** tab of the incident snapshot includes an entry for each time the **Do Not Archive** or **Allow Archive** flags are set for the incident.

See "Filtering reports" on page 1021.

Access to archiving functionality is controlled by roles. You can set the following user privileges on a role to control access:

- Archive Incidents—Grants permission for a user to archive incidents.
- Restore Archive Incidents—Grants permission for a user to restore archived incidents.
- Remediate Incidents—Grants permission for a user to set the Do Not Archive or Allow Archive flags.

See "About role-based access control" on page 84.

See "Archiving incidents" on page 1066.

See "Restoring archived incidents" on page 1066.

See "Preventing incidents from being archived" on page 1067.

## Archiving incidents

#### To archive incidents

- Open the Enforce Server administration console and navigate to an incident report.
- Select the incidents you want to archive, either by selecting the incidents manually or by setting filters or advanced filters to return the set of incidents that you want to archive.
- 3 Click the Incident Actions button and select Archive > Archive Incidents. The selected incidents are archived.

## Restoring archived incidents

#### To restore archived incidents

- Open the Enforce Server administration console and navigate to an incident report.
- Select the Advanced Filters & Summarization link. 2
- 3 Click the **Add filter** button.

- Select **Is Archived** in the first drop-down list.
- 5 Select **Show Archived** from the second drop-down list.
- Select the incidents you want to restore, either by selecting incidents manually or by setting filters or advanced filters to return the set of incidents you want to restore.

The selected incidents are restored.

## Preventing incidents from being archived

You can prevent incidents from being archived using either an incident report or an incident snapshot.

#### To prevent incidents from being archived using an incident report

- Open the Enforce Server administration console and navigate to an incident report.
- 2 Select the incidents you want to prevent from being archived. You can select incidents manually or by setting filters or advanced filters to return the set of incidents you want to prevent from being archived.
- 3 Click the Incident Actions button and select Archive > Do Not Archive.

The selected incidents are prevented from being archived.

Note: You can allow incidents to be archived that you have prevented from being archived by selecting the incidents and then selecting Archive > Allow Archive from the Incident Actions button.

#### To prevent an incident from being archived using the incident snapshot

- 1 Open the Enforce Server administration console and navigate to an incident report.
- 2 Click on an incident to open the incident snapshot.
- 3 On the **Key Info** tab, in the **Incident Details** section, click **Do Not Archive**.

Note: You can allow an incident to be archived that you have prevented from being archived by opening the incident snapshot and then clicking Allow Archive in the Incident Details section.

## **Deleting archived incidents**

#### To delete archived incidents

- Open the Enforce Server administration console and navigate to an incident report.
- 2 Click the Advanced Filters & Summarization link.
- 3 Click Add filter.
- 4 Select Is Archived in the first drop-down list.
- 5 Select **Show Archived** from the second drop-down list.
- Select the incidents you want to delete. You can select the incidents manually or you can set filters or advanced filters that return the set of incidents you want to delete.
- 7 Click the **Incident Actions** button and select **Delete incidents**.
- 8 Select one of the following delete options:

Delete incident completely	Permanently deletes the incident(s) and all associated data (for example, any emails and attachments). Note that you cannot recover the incidents that have been deleted.
Retain incident, but delete message data	Retains the actual incident(s) but discards the Symantec Data Loss Prevention copy of the data that triggered the incident(s). You have the option of deleting only certain parts of the associated data. The rest of the data is preserved.
Delete Original Message	Deletes the message content (for example, the email message or HTML post). This option applies only to Network incidents.

## Delete

This option refers to files (for Endpoint and Discover incidents) or Attachments/Files email or posting attachments (for Network incidents). The options are All, which deletes all attachments, and Attachments with no violations. For example, choose this option to delete files (for Endpoint and Discover incidents) or email attachments (for Network incidents).

> This option deletes only those attachments in which Symantec Data Loss Prevention found no matches. For example, choose this option when you have incidents with individual files taken from a compressed file (Endpoint and Discover incidents) or several email attachments (Network incidents).

9 Click the **Delete** button.

## Chapter

# Working with incident data

This chapter includes the following topics:

- About incident status attributes
- Configuring status attributes and values
- Configuring status groups
- Export web archive
- Export web archive—Create Archive
- Export web archive—All Recent Events
- About custom attributes
- About using custom attributes
- How custom attributes are populated
- Configuring custom attributes
- Setting the values of custom attributes manually

### About incident status attributes

Incident status attributes are specified and configured from the **Attributes** screen (**System > Incident Data > Attributes**).

Any status attribute listed on this screen can be assigned to any given incident by selecting it from the incident snapshot **Status** drop-down menu.

The system attributes page contains the following attributes to assist in incident remediation:

Status Values

The **Status Values** section lists the current incident status attributes that can be assigned to a given incident. Use this section to create new status attributes, modify them, and change the order that each attribute appears in drop-down menus.

See "Configuring status attributes and values" on page 1071.

#### Status Groups

The **Status Groups** section lists the current incident status groups and their composition. Use this section to create new status groups, modify them, and change the group order they appear in drop-down menus.

See "Configuring status groups" on page 1072.

#### Custom Attributes on the Custom Attributes tab

The Custom Attributes tab provides a list of all of the currently defined custom incident attributes. Custom attributes provide information about the incident or associated with the incident. For example, the email address of the person who caused the incident, that person's manager, why the incident was dismissed, and so on. Use this tab to add, configure, delete, and order custom incident attributes.

See "About custom attributes" on page 1076.

The process for handling incidents goes through several stages from discovery to resolution. Each stage is identified by a different status attribute such as "New," "Investigation," "Escalated," and "Resolved." This lets you track the progress of the incident through the workflow, and filter lists and reports by incident status.

The solution pack you installed when you installed Symantec Data Loss Prevention provides an initial default set of status attributes and status attribute groups. You can create new status attributes, or modify existing ones. The status attribute values and status groups you use should be based on the workflow your organization uses to process incidents. For example, you might assign all new incidents a status of "New." Later, you might change the status to "Assigned," "Investigation," or "Escalated." Eventually, most incidents will be marked as "Resolved" or as "Dismissed."

For list and report filtering, you can also create status groups.

Based on the preferences of your organization and the commonly used terminology in your industry, you can:

- Customize the names of the status attributes and add new status attributes.
- Customize the names of the status groups and add new status groups.
- Set the order in which status attributes appear on the Status drop-down list of an incident.
- Specify the default status attribute that is automatically assigned to new incidents.

See "Configuring status attributes and values" on page 1071.

See "About incident reports" on page 1009.

See "About incident remediation" on page 940.

See "About custom attributes" on page 1076.

## Configuring status attributes and values

As incidents are processed from discovery to resolution, each stage can be marked with a different status. The status lets you track the progress of the incident through your workflow. Based on the preferences of your organization and the commonly used terminology in your industry, you can define the different statuses that you want to use for workflow tracking.

The **Status Values** section lists the available incident status attributes that can be assigned to a given incident. The order in which status attributes appear in this list determines the order they appear in drop-down menus used to set the status of an incident. You can perform the following actions from the **Status Values** section:

Action	Procedure
Create a new incident status attribute.	Click the <b>Add</b> button.
Delete an incident status attribute.	Click the attribute's red X and then confirm your decision.
Change an incident status attribute.	Click on the attribute you want to change, enter a new name, and click <b>Save</b> .
	To change the name of an existing status, click on the pencil icon for that status, enter the new name, and click <b>Save</b> .
Make an incident status attribute the default.	Click <b>[set as default]</b> for an attribute to make it the default status for all new incidents.
Change an incident status attribute's order in drop-down menus.	<ul><li>Click [up] to move an attribute up in the order.</li><li>Click [down] to move an attribute down in the order.</li></ul>

#### To create a new incident status attribute

- Go to the Attributes screen (System > Incident Data > Attributes) screen. Click the Status tab.
- 2 Click the Add button in the Status Values section.

- 3 Enter a name for the new status attribute.
- Click Save.

See "Configuring status groups" on page 1072.

See "About incident status attributes" on page 1069.

## **Configuring status groups**

Incident status attributes can be assigned to status groups that match the workflow of your organization. For example, an **Open** status group might include the status attributes of New, Investigation, and Escalated. You can then filter incident lists and reports based on their status group. For example, you can list all incidents with status attributes that belong to the **Open** status group.

System > Incident Data > Attributes brings you to Status Groups.

For your convenience, you can group incident statuses to match the workflow of your organization. You use Status Groups to add or modify the name of a status group, and specify which status values to include in the group.

The **Status Groups** section lists the available incident status groups that can be used to filter incidents. For each group, the status attributes included in the group are listed. You can perform the following actions from the **Status Values** section:

Action	Procedure
Create a new incident status group.	Click the Add Status Group button.
Delete an incident status group.	Click the group's red X and then confirm your decision.
Change the name or incident status attributes of a group.	Click on the group you want to change. Click the pencil icon. Change the name, check or uncheck attributes, and click <b>Save</b> .
Change a status group's order in drop-down menus.	<ul><li>Click [up] to move a group up in the order.</li><li>Click [down] to move a group down in the order.</li></ul>

#### To define a new status group

- Go to the Attributes screen (System > Incident Data > Attributes) screen. Click the Status tab.
- 2 Click the Add Status Group button in the Status Groups section.
- 3 Enter a name for the new status group.

Click the check boxes for the status attributes that you want to include in this group.

Status attributes are defined with the **Add** button in the **Status Values** section.

See "Configuring status attributes and values" on page 1071.

Click Save. 5

See "Configuring status attributes and values" on page 1071.

See "About incident status attributes" on page 1069.

## **Export web archive**

Use this screen to save an incident list report as an archive of HTML pages. An archive allows personnel without direct access to Symantec Data Loss Prevention to study incident data, drilling down into individual incidents as needed.

When you export incidents as a Web Archive, the archive is placed in directory \SymantecDLP\Protect\archive\webarchive.

Note: You cannot archive summary reports or dashboards.

When exporting incidents, please note the following considerations:

- An archive cannot be summarized like a normal report.
- An archive contains no filters, so it may be difficult to locate a specific incident in an archive containing a large number of incidents.
- Exporting an archive of incidents does not remove the incidents from the administration console.
- You can export only one archive at a time.

Export Web Archive is a user privilege that must be assigned to a role. You can export web archives only if your role provides access to this feature. Since role access also determines what information is contained in incident reports, it also applies to archiving those incident reports. The information that is contained in the archive you create is the same information contained in the original incident report.

See "About configuring roles and users" on page 88.

The Export web archive screen is divided into two sections:

See "Export web archive—Create Archive" on page 1074.

See "Export web archive—All Recent Events" on page 1076.

## **Export web archive—Create Archive**

In the Create Archive section, complete the following information:

Field	Description
Archive Name	Specify a name for the archive you are creating using normal Windows naming conventions.

#### Field

#### Report to Export

#### Description

From the drop-down list, select the report that you want to archive. Any reports you created are available along with default report options.

The Network options are as follows:

- Incidents Week, Current—Network incidents from the current week.
- Incidents All—All network incidents.
- Incidents New-Network incidents with status of New.

The **Endpoint** options are as follows:

- Incidents Week, Current—Endpoint incidents from the current week.
- Incidents All—All endpoints incidents.
- Incidents New—Only endpoint incidents with status of New.

The **Discover** options are as follows:

- Incidents Last Scan—Discover incidents from the last completed scan. (Incidents from a currently active scan are not included.)
- Incidents Scan in Process—Discover incidents from the current scan.
- Incidents All Scans—All Discover incidents.
- Incidents New—Discover incidents with status of New.

The Mobile options are as follows:

- Incidents Week, Current—Network incidents from the current week.
- Incidents All—All network incidents.
- Incidents New-Network incidents with status of New.

The Classification options are as follows:

Events - All

After you complete the fields, click **Create** to compile the archive.

See "Export web archive" on page 1073.

## **Export web archive—All Recent Events**

The All Recent Events section displays a list of events related to this archive. (The list appears only after you click Create to create the archive.) Event entries show the following information:

- The event type (Error, Warning, or System Information).
- The event date and time
- A brief description of the event

To see the details of any event, click on the event entry in the list. To see the full Events Report for this archive, click show all.

See "Export web archive" on page 1073.

### About custom attributes

"Custom attributes" are incident data fields that provide a way to capture and store supplemental incident information. The additional data that is contained in custom attributes can be:

- Used to drive workflow.
- Execute incident response actions.
- Used in report metrics.
- Enable Incident Response Teams to act faster on incidents.
- Enable increased remediation and report automation.

You create the custom attributes that you need for these purposes. Custom attributes provide information about an incident or associated with an incident; for example, the email address of the person who caused the incident, that person's manager, why the incident was dismissed, and so on.

The Custom Attributes tab of the Attributes screen (System > Incident Data > Attributes) is used for working with custom attributes. The Attributes screen contains the following tabs:

- Status. The Status tab provides a list of all of the currently defined incident status attributes and status attribute groups. Use this tab to add, configure, delete, and order incident status attributes and incident status groups. See "About incident status attributes" on page 1069.
- Custom Attributes. The Custom Attributes tab provides a list of all of the currently defined custom incident attributes. Use this tab to add, configure, delete, and order custom incident attributes.

The solution pack you loaded when you installed Symantec Data Loss Prevention provides an initial default set of custom attributes. The Custom Attributes tab provides a list of all of the currently defined custom attributes that may be applied to any incident. This tab is for creating, modifying, and deleting custom attributes for your installation as a whole. Applying any of these custom attributes, or attribute values, to an individual incident is done from the incident snapshot, or by using a lookup plug-in.

On the **Custom Attributes** tab, you can perform the following functions:

Action	Procedure
Create a new custom attribute.	Click the <b>Add</b> button.
Delete a custom attribute.	Click the attribute's red "X" and then confirm your decision.
	Note that you cannot delete a custom attribute that is currently assigned to one or more incidents. You must assign a different attribute to the affected incident(s) before you can delete the custom attribute successfully.
Change the name, email status, or attribute group of an attribute.	Click on the attribute you want to change, change its parameters, and Click <b>Save</b> .
Change the attributes order in	1 Click [up] to move an attribute up in the order.
drop-down menus.	2 Click [down] to move an attribute down in the order.
Reload Lookup Plugins	Click <b>Reload Lookup Plug-ins</b> to reload any custom attribute plug-ins that have been unloaded by the system.
	Reloading look-up plugins affects all incidents. You may need to reload lookup plug-ins if any of the following are true:
	<ul> <li>A plug-in was problematic and the system unloaded it, but now the problem is fixed.</li> <li>The network was down or disconnected for some reason, but it is functioning properly now.</li> <li>A plug-in stores data in a cache, and you want to update the cache manually.</li> </ul>

See "About incident status attributes" on page 1069.

See "Configuring custom attributes" on page 1079.

See "Setting the values of custom attributes manually" on page 1080.

## About using custom attributes

When an incident is created, the Enforce Server retrieves data regarding that incident. Some of that data is in the form of "attributes." See the Symantec Data Loss Prevention Administration Guide for more information about incident attributes.

"Custom attributes" are a particular kind of attribute that is used to capture and store supplemental data. This data is related to the incident such as the name of a relevant manager or department. You create the custom attributes that you need.

The additional data that is contained in custom attributes can be used for:

- Enabling a workflow
- Executing incident response actions
- Including in report metrics
- Enabling incident response teams to act faster on incidents
- Enabling increased remediation and report automation

## How custom attributes are populated

For each incident, custom attributes can be populated (their values can be set in the incident data) in the following ways:

- Automatically when the incident is detected by means of a lookup plug-in, as described in this guide
- Automatically when the incident is detected by means of an automated response rule
- Automatically when a user executes a Smart Response Rule
- Manually (through data entry) by specific users after detection

Custom attributes can also be re-populated automatically by clicking on the **Lookup** option in the Attribute section of the Incident Snapshot screen. This action replaces the existing values that are stored in the custom attribute fields with the values returned by the new lookup.

Note: If the new lookup returns null or empty values for any custom attribute fields, those empty values overwrite the existing values.

## Configuring custom attributes

Use the Configure Custom Attribute screen to add or modify the a custom attribute.

Custom attributes can be grouped into attribute groups, similar to how statuses are grouped into status groups, to organize the information in a useful way. Examples of common attribute groups include Employee Information, Manager Information, and **Remediation Information**. All custom attributes are available for all incidents.

#### To create custom attributes and add them to a group

- On the Enforce Server, click System > Incident Data > Attributes > Custom Attributes. Note that a number of custom attributes were defined and loaded for you by the Solution Pack that you selected during installation. All existing custom attributes are listed in the Custom Attributes window.
- 2 To create a new custom attribute, click the **Add** option.
- Type a name for the custom attribute in the **Name** box. If appropriate, check the Is Email Address box.
  - The name you give to a custom attribute does not matter. But a custom attribute you create must be structured the same as the corresponding external data source. For example, suppose an external source stores department information as separate geographic location and department name. In this case, you must create corresponding location and department name custom attributes. You cannot create a single department ID custom attribute combining both the location and the department name.
- Select an attribute group from the **Attribute Group** drop-down list. If necessary, create a new attribute group. Select Create New Attribute Group from the drop-down list, and type the new group name in the text box that appears.
- 5 Click the **Save** option.
- 6 Generate a new incident, or view an existing incident, and verify that it contains the new custom attribute.

Once you define your custom attributes, they become available to every incident. Each incident receives its own set of custom attributes (though some name-value pairs may be empty depending on circumstances). The custom attribute values for an incident can be populated and changed independently of other incidents.

You can edit the custom attribute values if you have been assigned to a role that includes edit access for custom attributes. If you want to update a group of incidents, you can select those incidents on the incident list page. You can then select the Set Attributes command from the Incident Actions menu. You can select Lookup Attributes, to look up the values of custom attributes. Note that the Set Attributes command and Attributes section on the Incident Snapshot page are available only if at least one custom attribute is defined.

See "Configuring custom attributes" on page 1079.

See "About incident status attributes" on page 1069.

See "Configuring status groups" on page 1072.

See "Configuring status attributes and values" on page 1071.

## Setting the values of custom attributes manually

You can manually specify incident remediation status or workflow progress with values in custom attributes.

Note: To auto-populate custom attribute values, use one or more lookup plugins. See "About lookup plug-ins" on page 1092.

#### To set the value of custom attributes

- 1 Display an incident snapshot.
- 2 Click the **Edit** option in the **Attributes** section of the incident snapshot.
- 3 To set a value for a custom attribute, enter the value in the appropriate attributes field.
- When you are finished setting values, click Save.

# Working with user risk

This chapter includes the following topics:

- About user risk
- About user data sources
- Viewing the user list
- Viewing user details
- Working with the user risk summary

# About user risk

The user risk summary gives you insight into the behavior of specific individuals in your organization by associating users with email and endpoint incidents. This information helps you focus your data loss prevention efforts on those users posing the highest risk to the security of your data.

The Table 49-1 table provides and overview of the steps for creating and working with user risk summary reports.

Table 49-1 User Risk Summary workflow

Step	Action	Description
1	Create custom user attributes	You can create custom attributes for filtering and working with user risk summary reports. For example, you can create an attribute named Employment Status to track the employment status of each of your users. You can then import that information in a file that is exported from your enterprise resource planning system, such as PeopleSoft See "Defining custom attributes for user data" on page 1084.

**Table 49-1** User Risk Summary workflow (continued)

Step	Action	Description
2	Import user data	You can import user data from an Active Directory connection or from a CSV file. Incidents are associated with specific users by email address and login credentials. You can also upload files with your custom attributes, such as information from your enterprise resource planning system. Symantec Data Loss Prevention provides a CSV template file that you can use to format any data you want to upload. See "Bringing in user data" on page 1084.
3	View the <b>User List</b>	The <b>User List</b> is a list of all users in your system, including their email address, domain, and login name.
		See "Viewing the user list" on page 1090.
		You can view details for specific users in the user snapshot.
		See "Viewing user details" on page 1090.
4	View the User Risk Summary	The <b>User Risk Summary</b> displays your users and their associated Endpoint and Network incidents. Use the <b>User Risk Summary</b> to drill into your user-centric incident data to help you find the highest-risk users. You can sort and filter this list by policies, custom attributes, incident status, incident severity, number of incidents, date, incident type, and user name.
		See "Working with the user risk summary" on page 1091.
5	Export user risk summary or user snapshot data.	You can export data from the user risk summary and user snapshots to a CSV file.
		See "Working with the user risk summary" on page 1091.
		See "Viewing user details" on page 1090.

Using the information that is provided in the user risk summary, you can see who the high-risk users are and determine the appropriate course of action to take. Such actions might include:

- Determining whether or not a user poses an active threat to your data security.
- Applying additional policies to monitor a user's behavior more closely.
- Applying additional response rules to block actions or send alerts.
- Escalating a user's behavior to their manager or other responsible party.

To work with user risk data, a Symantec Data Loss Prevention user must have the User Reporting privilege. Be aware that users with this privilege are automatically able to view and access all incidents and incident types in Symantec Data Loss

Prevention. The user risk summary is intended for use by high-level remediators or information security officers. This privilege is not part of any predefined role.

See "Configuring roles" on page 91.

# About user data sources

You can bring in data about your users in CSV file format or through an Active Directory connection.

User data is information about people in your organization who may have access to data that you want to keep secure. To track user risk, you must provide the user's first and last name, their email address (to track Network incidents) and login information (to track Endpoint incidents). You can also provide additional standard directory attribute information, such as the user's address and phone number, as well as custom attributes such as the user's employment status.

The Table 49-2 table lists the required and optional standard user data attributes:

**Table 49-2** Standard user data

Attribute	Required or optional	Description
FIRST_NAME	Required	The user's given name.
LAST_NAME	Required	The user's surname.
EMAIL	Required if no login information is included	The user's email address.
LOGIN	Required if no email address is included	The user's login information, in DOMAIN\LOGIN format
TELEPHONE_NUMBER	Optional	The user's telephone number.
EMPLOYEE_ID	Optional	The user's employee identification number.
TITLE	Optional	The user's job title.
DEPARTMENT	Optional	The user's job department.
STREET_ADDRESS	Optional	The user's street address
STATE_OR_PROVINCE	Optional	The state or province in which the user resides.
COUNTRY	Optional	The country in which the user resides.
POSTAL_CODE	Optional	The postal code for the user's address.

See "Defining custom attributes for user data" on page 1084.

See "Bringing in user data" on page 1084.

# Defining custom attributes for user data

You can create custom attributes to improve relevance while filtering and working with user risk summary reports. Useful custom attributes might include employment status, the name of the user's manager, the user's job function, and other information that might be stored in your enterprise resource planning system or additional user data source.

You must create custom attributes before entering any user data. Each custom attribute is assigned a unique identification number as it is created. You must add these custom attribute identification numbers to your data file before you import it to Symantec Data Loss Prevention.

See "Adding a file-based user data source" on page 1085.

## To define custom attributes for user data

- In the Enforce Server administration console, go to System > Users > Attributes.
- 2 Click Add. The User Attribute dialog box appears.
- Enter the custom attribute in the **Name** field. The custom attribute can be a maximum of 60 characters.
- Click Submit.

### To view and edit user custom attributes

- In the Enforce Server administration console, go to **System > Users >** Attributes.
- The custom attributes appear in the **User Custom Attributes** list. You can take these actions:
  - To filter the User Custom Attributes list, click Filters, then use the text fields for ID or Attribute Name to enter a filter value.
  - To edit a custom attribute, click the attribute name or click the edit icon in the **Actions** column, then edit the attribute in the **User Attribute** dialog box.
  - To delete a custom attribute, click the delete icon in the Actions column.

# Bringing in user data

You can bring in user data from a file or an Active Directory connection.

See "Adding a file-based user data source" on page 1085.

See "Adding an Active Directory user data source" on page 1086.

After you have added your user data sources, you can schedule Symantec Data Loss Prevention to regularly import data from those data sources to ensure that your user data is always up to date. You can also import a user data source manually.

See "Importing a user data source" on page 1088.

## Adding a file-based user data source

You can bring in user data from a .csv file. For your convenience, Symantec Data Loss Prevention provides an annotated .csv template that you can use to ensure that your data is formatted correctly. The template includes all the standard user attributes, as well as formatting examples and instructions for adding custom attributes. The template also includes headers for any custom attributes that you have defined at the time you download the template.

## To create a user data file from a template

- In the Enforce Server administration console, go to System > Users > Data Sources.
- 2 On the Data Sources page, click **Download CSV Template** on the right-hand side of the page.
- Open the template file and provide the information for the standard user-data attributes.
  - See "About user data sources" on page 1083.
- The template file includes column headers for any custom attributes you have defined.
  - To add custom attributes manually, create a new column for each attribute, then populate the rows as appropriate.
  - You must enter the column headers in this format: ID[Attribute Name]. For example, 1[Employment Status].
  - See "Defining custom attributes for user data" on page 1084.
- 5 Save the file (in .csv format) to a location on your Enforce Server.

## To add a file-based user data source

- 1 In the Enforce Server administration console, go to **System > Users > Data** Sources.
- 2 On the Data Source Management page, click Add > CSV User Source. The Add CSV User Source dialog box appears.
- 3 In the **Add CSV User Source** dialog box, enter the following information:
  - Name: Specify a name for the data source.
  - File Path: Specify the path to the user data file. This file must be on the Enforce Server.
  - Delimited by: Specify the delimiter for the file. Valid delimiters are comma, pipe, semicolon, and tab.
  - Encoded by: Specify the character encoding format.
  - **Error Threshold Percentage:** Specify the percentage of user records that can be invalid before the file is rejected and the import process fails. Records with duplicate email addresses or logins count against the error threshold.
- Click Submit.

# Adding an Active Directory user data source

You can use an existing Active Directory connection to bring in user data. To add custom attributes for users that are added from an Active Directory source, create and import a data user file that includes the users' first and last names, email or login information, and the custom attributes you want to use. Symantec Data Loss Prevention automatically associates the file-based user data with the existing user records brought in from your Active Directory source.

Symantec Data Loss Prevention uses this Active Directory filter to retrieve user data (line breaks added for readability):

```
(&
 (objectClass=user)
 (objectCategory=person)
 (sAMAccountType=805306368)
 (!
  (|
   (&
    (sAMAccountType=805306368)
    (sAMAccountName=-*)
   )
   (&
```

```
(sAMAccountType=805306368)
    (sAMAccountName= *)
   )
  )
 )
)
```

Your Active Directory credentials must have permission to access the following user attributes:

```
FIRST NAME givenName
LAST NAME sn
{\it EMAIL} mail
LOGIN NAME sAMAccountName
TELEPHONE telephoneNumber
TITLE title
COUNTRY co
DEPARTMENT department
EMPLOYEE ID employeeId
STREET ADDRESS streetAddress
LOCALITY NAME 1
POSTAL CODE postalCode
STATE OR PROVINCE st
OBJECT DISINGUISHED NAME distinguishedName
```

Your Active Directory credentials must also have permission to access the RootDSE record. Symantec Data Loss Prevention reads these attributes from RootDSE:

```
namingContexts
defaultNamingContext
rootDomainNamingContext
configurationNamingContext
schemaNamingContext
isGlobalCatalogReady
highestCommittedUSN
```

See "Configuring directory server connections" on page 127.

See "Defining custom attributes for user data" on page 1084.

See "Adding a file-based user data source" on page 1085.

## To add an Active Directory user data source

- In the Enforce Server administration console, go to System > Users > Data Sources.
- 2 On the Data Source Management page, click Add > AD User Source. The Add AD User Source dialog box appears.
- 3 In the **Add > AD User Source** dialog box, enter the following information:
  - Name: Specify a name for the data source.
  - **Directory Connection:** Select an existing Active Directory connection.
  - Advanced Options > AD Custom Filter: Specify an optional filter for your Active Directory user data source, such as a workgroup. For example:

```
(& (region=North America) (!systemAccount=true))
```

## Click Submit.

Note: Best practices suggest that you should refer to directory connection objects with baseDNs in the user section of your directory tree. For example:

ou=Users, dc=corp, dc=company, dc=com.

# Importing a user data source

After you have added your user data sources, you can schedule Symantec Data Loss Prevention to regularly import data from those data sources to ensure that your user data is always up to date. You can also import a user data source manually.

Records with duplicate logins or email addresses are excluded from user data source imports. The number of records excluded from the import is displayed at the end of the import process, and the duplicate information appears in the logs.

To view details for a user data source import, click the **Status** link.

## To schedule import of a user data source.

- In the Enforce Server administration console, go to System > Users > Data Sources.
- 2 On the **Data Source Management** page, click the **Schedule** icon for your desired data source.
- Choose one of these options for scheduling: 3
  - Once: Specify a single day and time for user data import.
  - Daily: Specify a time for daily import of the user data source.

- Weekly: Specify a day and time for weekly import of the user data source.
- **Monthly:** Specify a day and time for monthly import of the user data source.
- Click Submit.

## To import a data source manually

- In the Enforce Server administration console, go to System > Users > Data Sources.
- On the **Data Source Management** page, select the data source you want to import.
- 3 Click Import.

## To view data source import details

- In the Enforce Server administration console, go to System > Users > Data Sources.
- On the Data Source Management page, click the Status link for your desired data source.

The **Import Details** dialog box appears.

- 3 The **Import Details** dialog box displays the following information for all imports:
  - Name: the name of the imported data source.
  - Status: Done, Completed with Errors, Failed.
  - Queued at: the time that the data source import was entered in the import queue.
  - **Started at**: the start time of the data source import.
  - **Completed at**: the completion time of the data source import.

For successful imports and imports completed with errors, the Import Details dialog box displays the following additional information:

- Added records: the number of added user records
- **Updated records**: the number of updated user records
- **Skipped errored records**: the number of records skipped because of errors in the user data source
- Skipped duplicate records: the number of records skipped because of duplicate user data

For failed imports, the **Import Details** dialog box displays the following additional information:

- Last successful import: the date and time of the last successful import of the user data source
- **Failure reason**: the reason for the import failure

# Viewing the user list

The user list displays all users that you have entered in Symantec Data Loss Prevention. In the user list, you can view the names, email addresses, and domain and login information for each user. You can sort the list first or last name, and you can search the list by name, email address, domain, or login. Clicking on an individual user's name takes you to the user detail view.

See "Viewing user details" on page 1090.

The user list does not display incident data, only user data.

## To view the user list

- In the Enforce Server administration console, go to Incidents > Users > User List.
- 2 To sort the user list by first or last name, click one of the sort icons in the appropriate column.
- To search the user list, enter your search term in the search field at the upper-right corner of the list. You can search on the user's first and last name, login, and email address. Only one search term is handled at a time.

# Viewing user details

The user snapshot shows all user information and incidents for a specific user. You reach the user detail view by clicking a user's name on the user list. You can also export the user snapshot to a CSV file.

See "Viewing the user list" on page 1090.

## To view user details

- 1 In the Enforce Server administration console, go to Incidents > Users > User
- Click the name of the user for whom you want to view details.
- On the **User** page, you can view a list of incidents, as well as user information, standard attributes, and custom attributes.
- 4 To export the user snapshot to a CSV file, click **Export**.

# Working with the user risk summary

The user risk summary displays all users who have incidents associated with them. You can sort and filter the user risk summary to gain insight into the user risk in your organization. For example, you can view incidents that are associated with specific policies, or with custom attributes that you have entered, such as job function or employment status. If you want to return to a particular view of the user risk summary, you can save the URL and bookmark it in your web browser. You can also export data from the user risk summary to a CSV file.

## To view the user risk summary

- In the Enforce Server administration console, go to Incidents > Users > User Risk Summary.
- 2 To sort the list, click one of the sort icons in one of the columns.
- 3 To filter the list, select your filter values using the buttons above the user risk summary list:

Filter	Default value	Description
Policies	All	Select a policy or policies by expanding the policy group and checking the appropriate box or boxes.
Attributes	None (0)	Enter up to two custom attributes to filter the list. Select the attribute from the drop-down list, then specify an include or exclude condition and enter your desired values. To add a second attribute filter, click <b>Add Attribute Filter</b> .
Status	All	Filter the list by incident status.
Date	Last 7 Days	Filter the list by date or date range.
Туре	All	Filter the list by incident type, such as <b>Email/SMTP</b> , <b>Printer/Fax</b> , or <b>HTTP</b> .
Severity	All	Filter the list by incident severity. You must select at least one severity level.

- 4 After you have selected your filter values, click **Apply**.
- 5 To save a particular filter configuration, click **Get Link** and copy the provided URL to your web browser bookmarks.
- To export data from the user risk summary to a CSV file, click **Export**. You can export the current page or all pages in the user risk summary.

# Implementing lookup plug-ins

This chapter includes the following topics:

- About lookup plug-ins
- Implementing and testing lookup plug-ins
- Configuring the CSV Lookup Plug-In
- Configuring LDAP Lookup Plug-Ins
- Configuring Script Lookup Plug-Ins
- Configuring migrated Custom (Legacy) Lookup Plug-Ins

# About lookup plug-ins

A lookup plug-in lets you connect the Enforce Server to an external system to retrieve supplemental data related to an incident. The data is stored as attributes. Lookup plug-ins let you add additional context to incidents to facilitate remediation workflow. For example, consider an email message that triggers an incident. A lookup plug-in can be used to retrieve and display the name and the email address of the sender's manager from a directory server based on the email sender's address.

Lookup plug-ins use incident attributes and custom attributes in coordination with each other. The system generates incident attributes when a policy rule is violated. You define custom attributes for custom incident data. Continuing the example, on detection of the incident, the system generates the incident attribute "sender-email" and populates it with the email address of the sender. The lookup plug-in uses this key-value pair to look up the values for custom attributes "Manager Name" and

"Manager Email" from an LDAP server. The plug-in populates the custom attributes and displays them in the Incident Snapshot.

See "About custom attributes" on page 1076.

See "About using custom attributes" on page 1078.

See "How custom attributes are populated" on page 1078.

# Types of lookup plug-ins

Symantec Data Loss Prevention provides several types of lookup plug-ins, including CSV, LDAP, Script, Data Insight, and Custom (Legacy). The following table describes each type of lookup plug-in in more detail.

See "About lookup plug-ins" on page 1092.

Types of lookup plug-ins Table 50-1

Table 30-1 Types of lookup plug ins		
Туре	Description	
CSV	The CSV Lookup Plug-in lets you retrieve incident data from a comma-separated values (CSV) file uploaded to the Enforce Server. You can configure one CSV Lookup Plug-in per Enforce Server instance.	
	See "About the CSV Lookup Plug-In " on page 1094.	
LDAP	The LDAP Lookup Plug-in lets you retrieve incident data from a directory server, such as Microsoft Active Directory, Novell LDAP, Oracle Directory Server (formerly Sun ONE), or IBM LDAP. You can configure multiple instances of the LDAP Lookup Plug-in.	
	See "About LDAP Lookup Plug-Ins" on page 1094.	
Script	The Script Lookup Plug-in lets you write a script to retrieve incident data from any external resource. For example, you can use a Script Lookup Plug-in to retrieve incident data from external resources such as proxy log files or DNS systems. You can configure multiple instances of the Script Lookup Plug-in.	
	See "About Script Lookup Plug-Ins" on page 1094.	
Data Insight	The Data Insight Lookup Plug-in lets you retrieve incident data from Symantec Data Insight so that you can locate and manage data at risk. You can configure one Data Insight Lookup Plug-in per Enforce Server instance.	
Custom (Legacy)	The Custom (Legacy) Lookup Plug-in lets you use Java code to retrieve incident data from any external resource.	
	See "About Custom (Legacy) Lookup Plug-Ins" on page 1095.	
	<b>Note:</b> As the name indicates, the Custom (Legacy) Lookup Plug-in is reserved for legacy Java plug-ins. For new custom plug-in development, you must use one of the other types of lookup plug-ins.	

## About the CSV Lookup Plug-In

The CSV Lookup Plug-In extracts data from a comma-separated values (CSV) file stored on the Enforce Server. The plug-in uses data from the CSV file to populate custom attributes for an incident at the time the incident is generated.

The CSV Lookup Plug-In receives a group of lookup parameters that contain data about an incident from the Enforce Server. One or more of the lookup parameters in the group is mapped to column heads in a CSV file. For example, the sender-email lookup parameter might be mapped to the Email column in the CSV file. The value in the lookup parameter is used as a key to find a matching value in the corresponding CSV column. When a match is found, the CSV row that contains the matching value provides the data that is returned to the Enforce Server. The Enforce Server uses the data in that row to populate the custom attributes for that incident. For example, if the sender-email lookup parameter contains the value mary.smith@mycompany.com, the pluq-in searches the Email column for a row that contains mary.smith@mycompany.com. That row is then used to provide the data to populate the custom attributes for the incident.

The CSV Lookup Plug-In uses an in-memory database to process large files.

See "Configuring the CSV Lookup Plug-In" on page 1112.

# **About LDAP Lookup Plug-Ins**

The LDAP Lookup Pluq-In pulls data from a live LDAP system (such as Microsoft Active Directory, Novell LDAP, Oracle LDAP, or IBM LDAP). It then uses that data to populate custom attributes for an incident at the time the incident is generated.

The LDAP Lookup Plug-In receives a group of lookup parameters that contain data about an incident from the Enforce Server. These lookup parameters are then used in LDAP queries to pull data out of an existing LDAP directory. For example, the value of the sender-email lookup parameter might be compared to the values in the email attribute of the directory. If the sender-email lookup parameter contains mary.smith@mycompany.com, a query can be constructed to search for a record whose email attribute contains mary.smith@mycompany.com. Data in the record that the search returns is inserted into the custom attributes for the incident.

See "Configuring LDAP Lookup Plug-Ins" on page 1122.

# **About Script Lookup Plug-Ins**

You can write one or more Script Lookup Plug-ins to guery data repositories for attribute values. For example, you can write a script that queries a DNS server for information about a sender that is involved in an incident. A Script Lookup Plug-In can use the output from such scripts to populate custom attributes in incident records.

Unlike the CSV or LDAP Lookup Plug-ins, the Script Lookup Plug-In does not use in-line attribute maps to specify how to look up parameter keys. Instead, you write this functionality into each script as needed.

To implement a Script Lookup Plug-In, you can use any scripting language that reads standard input (stdin) and writes standard output (stdout). The examples in the user interface and in this documentation use Python version 2.6.

See "Configuring advanced plug-in properties" on page 1111.

## About the Data Insight lookup plug-in

The Symantec Data Insight lookup plug-in retrieves data from a Symantec Data Insight Management Server and uses it to populate attributes for a Network Discover incident at the time the incident is generated. The Data Insight lookup plug-in connects Symantec Data Loss Prevention with Symantec Data Insight to retrieve attribute values. Data Insight can be used to provide granular context to incidents, including up-to-date data owner information. The values for incident attributes are viewed and populated at the **Incident Snapshot** screen.

The Data Insight lookup plug-in requires a Data Insight license separate from Symantec Data Loss Prevention licensing. If your system is not licensed for Data Insight, the Data Insight lookup plug-in is not available. If you are licensed for Data Insight, refer to the Symantec Data Loss Prevention Data Insight Implementation Guide for details on integrating with Data Insight.

## About Custom (Legacy) Lookup Plug-Ins

You can use a Custom (Legacy) Lookup Plug-In to migrate legacy Custom Java Lookup Plug-Ins to the Enforce Server administration console. Because Custom Java Lookup Plug-Ins are no longer the preferred way to create new plug-ins, the information presented here is provided to support organizations using legacy plug-ins but upgrading to Data Loss Prevention version 12. As an alternative to migrating legacy Custom Java Lookup Plug-Ins, consider rewriting such plug-ins using a Script Lookup Plug-In or one of the other supported lookup plug-ins, such as CSV or LDAP.

See "Types of lookup plug-ins" on page 1093.

Note: Custom (Legacy) Lookup Plug-Ins should only be used for migrating legacy lookup plug-ins implemented using the Java Lookup API. Support for new Custom Java Lookup Plug-Ins are not supported.

See "Configuring migrated Custom (Legacy) Lookup Plug-Ins" on page 1138.

# About lookup parameters

When an incident is created, the Enforce Server generates incident attributes and populates them with data it captures from the incident. You use one or more incident attributes as lookup parameter keys to retrieve external data and populate custom attributes with values that have been retrieved from the external system. You choose which lookup parameters to use for your lookup plug-ins at the **Lookup Parameters** screen. At least one lookup parameter must be present in the external data source for the lookup to be performed.

While some attributes are created for all incident types, others are specific to the incident type. For example, the incident attribute sender-email is specific to SMTP incidents. Attributes specific to Endpoint and Discover incidents are prefaced by an identifier, such as discover-name and endpoint-machine-name. For administrative convenience, lookup parameters are organized into groups. An incident exposes all of the lookup parameters in each lookup parameter group that is enabled. On lookup, some of the name-value pairs in that group may be valueless depending on the type of incident. For example, the attribute value of the sender-email parameter is null for Discover incidents (sender-email=null).

Lookup plug-ins do not change the system-defined values of lookup parameters. The plug-in only uses these parameters as keys to perform the lookup and populate custom attributes. For example, if a lookup plug-in uses the subject lookup parameter, the value of this attribute is not changed by a value for this attribute in the external data source; the Enforce Server ignores the value after the lookup is made. There are two exceptions, however: data-owner-name and data-owner-email. These system-defined incident attributes function like custom attributes and their values are populated by retrieved values.

When you map the keys to your data source, the plug-in searches the keys in order until it finds the first matching value. When a matching value is located, the plug-in stops searching for the keys. The plug-in uses the data in the row that contains the first matching value to populate the relevant custom attributes. Therefore, key values are not used in combination, but rather the first value that is found is the key. Because the plug-in stops searching after it finds the first matching value, the order in which you list the keys in your attribute mapping is significant. Refer to the individual attribute mapping topics and examples for nuances among the lookup plug-in attribute mapping syntax.

To perform a lookup, you must map at least one lookup parameter key to a field in your external data source. Each lookup parameter group that you enable is a separate database query for the Enforce Server to perform. All database queries are executed for each incident before lookup. To avoid the performance impact of unnecessary database queries, you should only enable attribute groups that your lookup plug-ins require.

Because the plug-in stops searching after it finds the first matching lookup parameter key-value pair, the order in which you list the keys in your attribute map is significant. Refer to the attribute mapping examples for the specific type of plug-in you are implementing.

See "Selecting lookup parameters" on page 1102.

# About plug-in deployment

A lookup plug-in is deployed by enabling it through the user interface. Each lookup plug-in must be enabled, even if there is only one. If multiple plug-ins are enabled, you chain them together and specify their order of execution.

The selected lookup parameter keys apply globally to all deployed lookup plug-ins. If plug-ins are reloaded, all deployed plug-ins are reloaded.

You can only deploy one CSV Lookup Plug-in and one Data Insight Lookup Plug-in per Enforce Server instance.

See "Enabling lookup plug-ins" on page 1107.

# About plug-in chaining

When you create a lookup plug-in, you map the lookup parameter keys and custom attributes to fields in the external data source. All deployed lookup plug-ins receive a reference to the same attribute map. This allows plug-ins to be chained together and executed in sequence.

In a lookup plug-in chain, the first plug-in uses the lookup parameters that are passed to it by the Enforce Server to look up attribute values. The second plug-in uses data that is passed to it by the first plug-in including the lookup parameters and any variables created by the previous lookup. This continues in sequence or all plug-ins in the chain.

A plug-in chain is useful when information must be pulled from different sources to populate custom attributes for an incident. A chain is also useful when there are differences or dependencies between the "keys" needed to unlock the correct data.

For example, consider the following plug-in chain:

- 1. A Script Lookup Plug-in performs a DNS lookup using one or more parameters.
- 2. A CSV Lookup Plug-in uses the result of the script look up to retrieve incident data from a CSV file that is an extract from an asset management system.

An LDAP Lookup Plug-in uses the result of the CSV lookup to obtain data from a corporate LDAP directory.

See "Chaining lookup plug-ins" on page 1108.

See "Chaining multiple Script Lookup Plug-Ins" on page 1134.

# About upgrading lookup plug-ins

Prior to Symantec Data Loss Prevention version 11.6, lookup plug-ins were implemented manually using property files; there was no user interface for configuring lookup plug-ins. The lookup plug-in user interface was introduced in version 11.6.

If you are upgrading to version 12.0 or later, existing lookup plug-ins are automatically upgraded to the new framework and added to the user interface for configuration and deployment. In addition, the plug-in state will be preserved after the upgrade, that is, if a plug-in was enabled before the upgrade it should be turned on in the user interface after the upgrade.

If the upgrade of a lookup plug-in does not succeed, the system displays the following error message:

```
INFO: IN PROCESS: Errors detected in lookup plugin configuration.
Your lookup plugins may require manual configuration after the upgrade.
```

In this case, check the plug-in at the System > Lookup Plugins screen and manually configure it following the instructions provided with this documentation. Refer to the Symantec Data Loss Prevention Release Notes for known issues related to the upgrade of lookup plug-ins.

# Implementing and testing lookup plug-ins

The following table describes the workflow for implementing and testing lookup plug-ins. Linked sections explain these steps in more detail.

Implementing and testing lookup plug-ins **Table 50-2** 

Step	Description
1	Decide what external data you want to extract and load into incidents as custom attributes.
	See "About using custom attributes" on page 1078.
2	Identify the sources from which custom attribute data is to be obtained and the appropriate lookup plug-in for retrieving this information.
	See "Types of lookup plug-ins" on page 1093.

Table 50-2 Implementing and testing lookup plug-ins (continued)

Step	Description
3	Create a custom attribute for each individual piece of external data that you want to include in incident snapshots and reports.
	See "Configuring custom attributes" on page 1079.
4	Determine which lookup parameter groups include the specific lookup parameters you need to extract the relevant data from the external sources.
	See "About lookup parameters" on page 1096.
5	Configure the plug-in to extract data from the external data source and populate the custom attributes.
	See "Configuring the CSV Lookup Plug-In" on page 1112.
	See "Configuring LDAP Lookup Plug-Ins" on page 1122.
	See "Configuring Script Lookup Plug-Ins" on page 1127.
	See "Configuring migrated Custom (Legacy) Lookup Plug-Ins" on page 1138.
6	Enable the plug-in on the Enforce Server.
	See "Enabling lookup plug-ins" on page 1107.
7	Set the execution order for multiple plug-ins.
	See "Chaining lookup plug-ins" on page 1108.
8	Verify privileges. The end user must have <b>Lookup Attribute</b> privileges to use a lookup plug-in to look up attribute values.
	See "Configuring roles" on page 91.
9	Generate an incident. The incident must be of the type that exposes one or more incident attributes that you have designated as parameter keys.
	See "Configuring policies" on page 326.
10	View the incident details. For the incident you generated, go to the <b>Incident Snapshot</b> screen. In the <b>Attributes</b> section, you should see the custom attributes you created. Note that they are unpopulated (have no value). If you do not see the custom attributes, verify the privileges and that the custom attributes were created.

Step	Description
11	If the lookup plug-in is properly implemented, you see the <b>Lookup</b> button available in the <b>Attributes</b> section of the <b>Incident Snapshot</b> . Once you click <b>Lookup</b> you see that the value for each custom attribute is populated. After the initial lookup, the connection is maintained and subsequent incidents will have their custom attributes automatically populated by that lookup plug-in; the remediator does not need to click <b>Lookup</b> for subsequent incidents. If necessary you can reload the plug-ins.
	See "Troubleshooting lookup plug-ins" on page 1109.

Table 50-2 Implementing and testing lookup plug-ins (continued)

# Managing and configuring lookup plug-ins

The System > Incident Data > Lookup Plugins screen is the home page for creating, configuring, and managing lookup plug-ins. Lookup plug-ins are used for remediation to retrieve incident-related data from an external data source and populate incident attributes.

See "About lookup plug-ins" on page 1092.

See "Reloading lookup plug-ins" on page 1108.

You create and configure lookup plug-ins at the Lookup Plugins List Page.

Creating and configuring lookup plug-ins Table 50-3

Action	Description
New Plugin	Select this option to create a new plug-in.
	See "Creating new lookup plug-ins" on page 1102.
Modify Plugin Chain	Select this option to enable (deploy) plug-ins and to set the order of lookup for multiple plug-ins.
	See "Enabling lookup plug-ins" on page 1107.
Lookup Parameters	Select this option to choose which lookup parameter groups to use as keys to populate attribute fields from external data sources.
	See "Selecting lookup parameters" on page 1102.
Reload Plugins	Select this option to refresh the system after making changes to enabled plug-ins or if the external data is updated. This action automatically performs the enabled lookups in order and populates the incidents as they are created.
	See "Reloading lookup plug-ins" on page 1108.

For each configured lookup plug-in, the system displays the following information at the Lookup Plugins List Page. You use this information to manage lookup plug-ins.

Table 50-4 Managing lookup plug-ins

Display field	Description
Execution Sequence	This field displays the order in which the system executes lookup plug-ins.
	See "Enabling lookup plug-ins" on page 1107.
Name	This field displays the user-defined name of each lookup plug-in.
	Click the <b>Name</b> link to edit that plug-in.
	See "Creating new lookup plug-ins" on page 1102.
Туре	The field displays the type of lookup plug-in. You can configure one CSV and one Data Insight Lookup Plug-in per Enforce Server instance. You can configure multiple instances of the LDAP, Script, and Custom (Legacy) lookup plug-ins.
	See "Types of lookup plug-ins" on page 1093.
Description	This field displays the user-defined description of each lookup plug-in.
	See "Implementing and testing lookup plug-ins" on page 1098.
Status	The field displays the state of each lookup plug-in, either <b>On</b> (green) or <b>Off</b> (red). To edit the state of a plug-in, click <b>Modify Plugin Chain</b> .
	See "Enabling lookup plug-ins" on page 1107.

For each configured lookup plug-in, you can perform the following management functions at the **Lookup Plugins List Page**.

Sorting and grouping lookup plug-ins Table 50-5

Action	Description
Edit	Click the pencil icon in the <b>Actions</b> column to edit the plug-in.
Delete	Click the X icon in the <b>Actions</b> column to delete the plug-in. You must confirm or cancel the action to execute it.
Sort	Sort the selected display column in ascending or descending order.
Group	Group the plug-ins according to the selected display column. For example, where you have multiple plug-ins, it may be useful to group them by <b>Type</b> or by <b>Status</b> .

# Creating new lookup plug-ins

You must have Server Administration privileges to create and configure lookup plug-ins.

See "Configuring roles" on page 91.

## To create new lookup plug-in

- Navigate to System > Incident Data > Lookup Plugins in the Enforce Server administration console.
- 2 Click **New Plugin** at the **Lookup Plugins List Page** screen.
- 3 Select the type of lookup plug-in you want to create and configure it.

## **CSV**

See "Configuring the CSV Lookup Plug-In" on page 1112.

### **LDAP**

See "Configuring LDAP Lookup Plug-Ins" on page 1122.

## Script

See "Configuring Script Lookup Plug-Ins" on page 1127.

## **Data Insight**

## Custom (Legacy)

See "Configuring migrated Custom (Legacy) Lookup Plug-Ins" on page 1138.

4 Click **Save** to apply the lookup plug-in configuration.

The system displays a success (green) message if the plug-in was successfully saved or an error (red) message if the plug-in is misconfigured and could not be saved.

See "Troubleshooting lookup plug-ins" on page 1109.

Click **Modify Plugin Chain** and enable the lookup plug-in and chain multiple plug-ins.

See "Enabling lookup plug-ins" on page 1107.

See "Chaining lookup plug-ins" on page 1108.

# Selecting lookup parameters

The System > Lookup Plugins > Edit Lookup Plugin Parameters page lists the **Lookup Parameter Keys** that you select to trigger the look up of attribute values. Lookup parameter keys are organized into attribute groups. Selections made at this screen apply to all lookup plug-ins deployed on the Enforce Server.

To perform a lookup, you must map at least one lookup parameter key to a field in your external data source. Each lookup parameter group that you enable is a separate database query for the Enforce Server to perform. All database queries are executed for each incident before lookup. To avoid the performance impact of unnecessary database queries, you should only enable attribute groups that your lookup plug-ins require.

Because the plug-in stops searching after it finds the first matching lookup parameter key-value pair, the order in which you list the keys in your attribute map is significant. Refer to the attribute mapping examples for the specific type of plug-in you are implementing for details.

See "About lookup parameters" on page 1096.

## To enable one or more lookup parameter keys

- Navigate to **System > Lookup Plugins** in the Enforce Server administration 1 console.
- 2 Click Lookup Parameters at the Lookup Plugins List Page.
- 3 Select (check) one or more attribute groups at the **Edit Lookup Plugin** Parameters page.

Click **View Properties** to view all of the keys for that attribute group.

- Attachment Table 50-6
- Incident Table 50-7
- Message Table 50-8
- Policy Table 50-9
- Recipient Table 50-10
- Sender Table 50-11
- Server Table 50-12
- Monitor Table 50-13
- Status Table 50-14
- ACI Table 50-15
- 4 Save the configuration.

Verify the success message indicating that all enabled plug-ins were reloaded.

Table 50-6 Attachment lookup parameters

Lookup parameter key	Description and comments
attachment-nameX	Name of the attached file, where X is the unique index to distinguish between multiple attachments, for example: attachment-name1, attachment-size1; attachment-name2, attachment-size2; etc.
attachment-sizeX	Original size of the attached file, where X is the unique index to distinguish between multiple attachments. See above example.

Incident lookup parameters **Table 50-7** 

Lookup parameter key	Description
date-detected	Date and time when the incident was detected, for example: date-detected=Tue May 15 15:08:23 PDT 2012.
incident-id	The incident ID assigned by Enforce Server. The same ID can be seen in the incident report. For example: incident-id=35.
protocol	The name of the network protocol that was used to transfer the violating message, such as SMTP and HTTP. For example: protocol=Email/SMTP.
data-owner-name	The person responsible for remediating the incident. This attribute is not populated by the system. Instead, it is set manually in the <b>Incident Details</b> section of the <b>Incident Snapshot</b> screen, or automatically using a lookup plug-in.
	Reports based on this attribute can automatically be sent to the data owner for remediation.
data-owner-email	The email address of the person responsible for remediating the incident. This attribute is not populated by the system. Instead, it is set manually in the <b>Incident Details</b> section of the <b>Incident Snapshot</b> screen, or automatically using a lookup plug-in.

**Table 50-8** Message lookup parameters

Lookup parameter key	Description
date-sent	Date and time when the message was sent if it is an email. For example: date-sent=Mon Aug 15 11:46:55 PDT 2011.
subject	Subject of the message if it is an email incident.
file-create-date	Date that the file was created in its current location, whether it was originally created there, or copied from another location. Retrieved from the operating system.

**Table 50-8** Message lookup parameters (continued)

Lookup parameter key	Description
file-access-date	Date that the file was examined.
file-created-by	User who placed the file on the endpoint.
file-modified-by	Fully-qualified user credential for the computer where the violating copy action took place.
file-owner	The name of the user or the computer where the violating file is located.
discover-content-root-path	Root of path of the file which caused a Discover incident.
discover-location	Full path of the file that caused a Discover incident.
discover-name	The name of the violating file.
discover-extraction-date	Date a subfile was extracted from an encapsulated file during Discover scanning.
discover-server	The name of repository to be scanned.
discover-notes-database	Specific attribute for Discover scan of Lotus Notes repository.
discover-notes-url	Specific attribute for Discover scan of Lotus Notes repository.
endpoint-volume-name	The name of the local drive where an endpoint incident occurred.
endpoint-dos-volume-name	The Windows name of the local drive where an endpoint incident occurred.
endpoint-application-name	Name of application most recently used to open (or create) the violating file.
endpoint-application-path	Path of the application that was used to create or open the violating file.
endpoint-file-name	The name of the violating file.
endpoint-file-path	Location the file was copied to.

**Table 50-9** Policy lookup parameter

Lookup parameter key	Description and comments
policy-name	The name of the policy that was violated, for example: policy-name=Keyword Policy.

Recipient lookup parameters Table 50-10

Lookup parameter key	Description
recipient-emailX	The email address of the recipient, where X is the unique index to distinguish between multiple recipients; for example: recipient-email1, recipient-ip1, recipient-url1; recipient-email2, recipient-ip2, recipient-url2; etc.
recipient-ipX	The IP address of the recipient, where X is the unique index to distinguish between multiple recipients. See above example.
recipient-urlX	The URL of the recipient, where X is the unique index to distinguish between multiple recipients. See above example.

#### **Table 50-11** Sender lookup parameters

Lookup parameter key	Description
sender-email	The email address of the sender for Network Prevent for Email (SMTP) incidents.
sender-ip	The IP address of the sender for Endpoint and Network incidents on protocols other than SMTP.
sender-port	The port of the sender for Network incidents on protocols other than SMTP.
endpoint-user-name	The user who was logged on to the endpoint when the violation occurred.
endpoint-machine-name	Name of the endpoint where the violating file resides.

Table 50-12 Server lookup parameters

Lookup parameter key	Description and comments
server-name	The name of the detection server that reported the incident. This name is user-defined and entered when the detection server is deployed. For example: server-name=My Network Monitor.

#### Monitor lookup parameters **Table 50-13**

Lookup parameter key	Description
monitor-name	The name of the detection server that reported the incident. This name is user-defined and entered when the detection server is deployed. For example: server-name=My Network Monitor.
monitor-host	The IP address of the detection server that reported the incident. For example: $monitor-host=127.0.0.1$

Table 50-13	Monitor	lookup	parameters	(continued)	
-------------	---------	--------	------------	-------------	--

Lookup parameter key	Description
monitor-id	The system-defined numeric identifier of the detection server. For example: monitor-id=1.

Table 50-14 Status lookup parameter

Lookup parameter key	Description and comments
incident-status	Current status of the incident. For example: incident-status=incident.status.New.

Table 50-15 ACL lookup parameters

Lookup parameter key	Description
acl-principalX	A string that indicates the user or group to whom the ACL applies.
acl-typeX	A string that indicates whether the ACL applies to the file or to the share.
acl-grant-or-denyX	A string that indicates whether the ACL grants or denies the permission.
acl-permissionX	A string that indicates whether the ACL denotes read or write access.

# Enabling lookup plug-ins

To enable a lookup plug-in you have to change its status from Off, which is the initial status of a plug-in after it is configured, to On. The System > Incident Data > Lookup Plugins > Modify Plugin Chain is where you enable lookup plug-ins.

See "About plug-in deployment" on page 1097.

## To enable a lookup plug-in

- Navigate to System > Incident Data > Lookup Plugins in the Enforce Server administration console.
- 2 Click Modify Plugin Chain at the Lookup Plugins List Page.
- 3 In the **Dedicated Actions** field, select (check) the **On** option.
- Click Save to apply the configuration.

If the plug-in cannot be loaded the system will report an error and the plug-in state will remain Off. In this case, check the latest Tomcat log file for the error.

See "Troubleshooting lookup plug-ins" on page 1109.

# Chaining lookup plug-ins

The System > Incident Data > Lookup Plugins > Modify Lookup Plugin **Execution Chain** is where you enable lookup plug-ins and specify the execution order when multiple lookup plug-ins are deployed.

See "Enabling lookup plug-ins" on page 1107.

If you enable multiple lookup plug-ins you must specify their order of execution. When plug-ins are chained together, input from a previous plug-in is used as attributes by subsequent lookup plug-ins.

See "About plug-in deployment" on page 1097.

## To chain multiple lookup plug-ins

- Navigate to System > Incident Data > Lookup Plugins in the Enforce Server administration console.
- 2 Click Modify Plugin Chain at the Lookup Plugins List Page.
- In the Execution Sequence field, select the execution order from the drop-down menu.
- Click **Save** to apply the chaining configuration.

# Reloading lookup plug-ins

If you have changed the configuration of a lookup plug-in, or the external data has changed, you need to reload the lookup plug-ins. Reloading plug-ins refreshes the system and automatically performs the enabled lookups in order and populates the incident attributes as incidents are detected.

In addition to reloading plug-ins if changes are made, you may need to reload lookup plug-ins if any of the following are true:

- A plug-in was problematic and the system unloaded it, but now the problem is fixed.
- The network was down or disconnected for some reason, but it is functioning properly now.
- A plug-in stores data in a cache, and you want to update the cache manually.

## To reload lookup plug-ins

- Navigate to **System > Incident Data > Lookup Plugins** in the Enforce Server administration console.
- 2 Click **Reload Plugins** to reload all enabled plug-ins.

Note: Administrators can also reload lookup plug-ins from the Custom Attributes tab of the System > Incident Data > Attributes screen.

# Troubleshooting lookup plug-ins

Symantec Data Loss Prevention provides logging and error messages specific to lookup plug-ins. The most common errors involve the failure of a plug-in to load due to one or more misconfigurations. If a lookup plug-in fails to load, the exception is logged as a warning at the system events screen and in the Tomcat log. In addition, the attribute map and plug-in execution chain is logged in the Tomcat log.

## To troubleshoot lookup plug-in errors

- Navigate to the **System > Servers > Overview** screen and look for any warnings in the Recent Error and Warning Events table at the bottom of the page.
- 2 On the Enforce Server host, open the log file \SymantecDLP\protect\Enforce\logs\tomcat\localhost.<date>.log.
- Troubleshoot errors that appear in the Tomcat localhost log file.

#### Table 50-16

- Configure detailed logging for lookup plug-ins if the plug-in fails but errors are not logged.
  - See "Configuring detailed logging for lookup plug-ins" on page 1110.
- 5 Refer to the troubleshooting topics for specific plug-ins.
  - See "Testing and troubleshooting the CSV Lookup Plug-In" on page 1118.
  - See "Testing and troubleshooting LDAP Lookup Plug-ins" on page 1125.
  - See "Script Lookup Plug-In tutorial" on page 1134.

Problem	Solution
Lookup plug-in fails to load	If the plug-in failed to load, search for a message in the log file similar to the following:
	SEVERE [com.vontu.enforce.workflow.attributes.AttributeLookupLoader] Error loading plugin [ <plugin_name>]  Note the "Cause" section that follows this type of error message. Any such entries will explain why the plug-in failed to load.</plugin_name>
Attributes are not populated by the lookup	If the plug-in loads but attributes are not populated, look in the log for the attribute map. Verify that values are being populated, including for the lookup parameters that you enabled. To do this, search for a lookup parameter key that you have enabled, such as sender-email.

Troubleshooting lookup plug-ins Table 50-16

# Configuring detailed logging for lookup plug-ins

The system provides detailed logging configuration for lookup plug-ins. You can configure the logging levels for lookup plug-ins in the System > Logs > Configuration tab. Configuring the logs for lookup plug-ins provides more detailed log messages in the Tomcat localhost log.

See "Troubleshooting lookup plug-ins" on page 1109.

To configure and collect the logs for lookup plug-ins

- Navigate to the **System > Servers > Logs** screen. 1
- 2 Select the **Configuration** tab.
- For the Enforce Server, select the Custom Attribute Lookup Logging entry from the Diagnostic Logging Setting drop-down menu.
- 4 Click Configure Logs.
- 5 In the Collection tab, select the following Debug and Trace Logs for the Enforce Server.
- 6 Click Collect Logs.
- At the bottom of the page, click **Download** to download the logs. Use the Refresh button to refresh the page. The logs are packaged in a ZIP file.
- 8 Open the ZIP file or save it to the file system and extract it.
- 9 Navigate to directory \SymantecDLPLogs.zip\Enforce\logs\tomcat.
- 10 Open the file localhost.<date>.log using a text editor. Open the file with the most recent date.

- 11 Search for the name of the lookup plug-in. You should see several messages.
- 12 If necessary, verify the lookup plug-in logging properties in file

\Protect\config\ManagerLogging.properties.

com.vontu.logging.ServletLogHandler.level=FINEST com.vontu.enforce.workflow.attributes.CustomAttributeLookup.level=FINEST com.vontu.lookup.level=FINEST

# Configuring advanced plug-in properties

The file SymantecDLP\protect\config\Plugins.properties contains several advanced properties for configuring lookup plug-ins. Generally these properties do not need to be modified unless necessary according to the following descriptions.

Advanced properties for lookup plug-ins Table 50-17

Property	Default	Description
AttributeLookup. output.parameters	data-owner-name, data-owner-email	The Attribute Lookup Output Parameters property is a comma-separated list that specifies which parameters can be modified by lookup plug-ins. Generally, the values for lookup parameter keys are set by the system when an incident is created. Because these parameters are used to look up custom attribute values, they are not modified by the looked up values if they are different from the system-defined values  However, this property lets you modify the output of the <b>Data Owner Name</b> and <b>Data Owner Email</b> attributes based on retrieved values. These parameters are specified in lookup plug-in configurations and scripts using the same syntax as custom attributes. Both attributes are enabled by selecting the <b>Incident</b> attribute group.  You can disable this feature by removing one or both of the entries. If removed, the output for either parameter is not changed by a looked up value.

Table 50-17 Advanced properties for lookup plug-ins (continued)

Property	Default	Description
AttributeLookup.timeout	60000	To avoid a system freeze due to unanticipated lookup problems, the Enforce Server limits the amount of time given to each lookup plug-in. This timeout is configured in the com.vontu.api.incident.attributes.AttributeLookup.timeout property in the Plug-ins.properties file.  If a lookup exceeds the 60-second default timeout, the incident attribute framework unloads the associated plug-in. If there is a runaway lookup the Enforce Server cannot execute that particular lookup for any subsequent incidents. If the plug-in times out frequently, you can extend the timeout by modifying the period (in milliseconds).  Note: Note that increasing this value may result in slower incident processing times because of slow attribute lookups.
AttributeLookup.auto	true	The automatic lookup property specifies whether the lookup should be triggered automatically when a new incident is detected. This property automatically populates incident attributes using the deployed lookup plug-ins after the initial lookup is executed. You can disable auto-lookup by changing the property value to false. If this property is disabled, remediators must click Lookup for every incident.  After setting the AttributeLookup.auto property to false, make sure you restart the Vontu Incident Persister service. If you do not restart the service the custom attributes will continue to be automatically populated.
AttributeLookup.reload	false	The automatic plug-in reload property specifies whether all plug-ins should be automatically reloaded each day at 3:00 A.M. Change to true to enable.

# Configuring the CSV Lookup Plug-In

You can only configure one CSV Lookup Plug-In per Enforce Server instance.

See "About the CSV Lookup Plug-In" on page 1094.

Configuring the CSV Lookup Plug-In Table 50-18

Step	Action	Description
1	Create custom attributes.	Define the custom attributes for the information you want to look up.
		See "Setting the values of custom attributes manually" on page 1080.
2	Create the CSV data source file.	The CSV file that contains the data to be used to populate custom attributes for incident remediation.
		See "Requirements for creating the CSV file" on page 1114.
3	Create a new CSV plug-in.	See "Creating new lookup plug-ins" on page 1102.
4	Name and describe the plug-in.	The name string limited to 100 characters. It is recommended that you enter a description for the lookup plug-in.
5	Specify the file path.	Provide the path to the CSV file. The CSV file must be local to the Enforce Server.
		See "Specifying the CSV file path" on page 1115.
6	Choose the File Delimiter.	Specify the delimiter that is used in the CSV file. The pipe delimiter [ ] is recommended.
		See "Choosing the CSV file delimiter" on page 1115.
7	Choose the File Encoding.	For example: UTF-8
		See "Selecting the CSV file character set" on page 1116.
8	Map the attributes.	Map the system and the custom attributes to the CSV file column heads and define the keys to use to extract custom attribute data. Keys map to column heads, not custom attributes.
		The syntax is as follows:
		attr.attribute_name=column_head
		keys=column_head_first:column_head_next:column_head_3rd
		See "Mapping attributes and parameter keys to CSV fields" on page 1116.
9	Save the plug-in.	Verify that the correct save message for the plug-in is displayed.
9	Select the Lookup Parameter Keys.	Define the keys which are used to extract custom attribute data.
		See "Selecting lookup parameters" on page 1102.
10	Enable the lookup plug-in.	The CSV Lookup Plug-In must be enabled on the Enforce Server.
		See "Enabling lookup plug-ins" on page 1107.
11	Troubleshoot the plug-in.	See "Testing and troubleshooting the CSV Lookup Plug-In" on page 1118.

Configuring the CSV Lookup Plug-In (continued) Table 50-18

Step	Action	Description
11	Test the lookup plug-in.	

# Requirements for creating the CSV file

The CSV Lookup Plug-In requires a CSV file that is stored on the Enforce Server. When creating a CSV file, keep in mind the following requirements:

- The first data row of the CSV file must contain column headers.
- Column header fields cannot be blank.
- Make sure that there are no white spaces at the end of the column header fields.
- Make sure that all rows have the same number of columns.
- Each row of the file must be on a single, non-breaking line.
- One or more columns in the file are used as key-fields for data lookups. You specify in the attribute mapping which column heads are to be used as key fields. You also specify the key field search order. Common key fields typically include email address, Domain\UserName (for Endpoint incidents), and user name (for Storage incidents).
- The data values in the key field columns must be unique. If multiple columns are used as key fields (for example, EMP EMAIL and USER NAME), the combination of values in each row must be unique.
- Fields in data rows (other than the column header row) can be empty, but at least one key field in each row should contain data.
- The same type of delimiter must be used for all values in the column header and data rows.
- If the CSV file is read-only, make sure that the CSV file has a new line at the end of the file. The system will attempt to add a new line to the file on execution of the plug-in, but if the file is read-only the system cannot do this and the plug-in will not load.
- For Discover scan incidents, the file-owner lookup parameter does not include a domain. To use file-owner as the key, the CSV file column that corresponds to file-owner should be in the format owner. The format DOMAIN\owner does not result in a successful lookup. This restriction only applies to Discover incidents, other kinds of incidents can include a domain.

For example, the column-header row and a data-row of a pipe-delimited CSV file might look like:

email|first name|last name|domain user name|user name|department|manager|manager email jsmith@acme.com|John|Smith|CORP\jsmith1|jsmith1|Accounting|Mei Wong|mwong@acme.com

- If more than 10% of the rows in the CSV file violate any of these requirements. the Plugin does not load.
- For accuracy in the lookup, the CSV file needs to be kept up to date.

See "About the CSV Lookup Plug-In" on page 1094.

# Specifying the CSV file path

To configure the CSV Lookup Plug-In you must specify the CSV File Path property for the location of the CSV file. The CSV file must be stored locally on the Enforce Server.

You can enter either an absolute file path or a relative file path. For example:

- ../../../symantecDLP csv lookup file/senders2.csv
- C:/SymantecDLP csv lookup file/senders2.csv

On Windows you can use either forward or backward slashes. For example:

C:/SymantecDLP/Protect/plugins/employees.csv Or

C:\SymantecDLP\Protect\plugins\employees.csv. On Linux you can only use forward slashes.

The system validates the file path when you save the configuration. If the system cannot locate the file it reports and error and does not let you save the configuration. Make sure that the CSV file is not open and is stored locally to the Enforce Server.

# Choosing the CSV file delimiter

Use the **Delimiter** property to specify the CSV file delimiter.

The following delimiters are supported:

- Comma
- Pipe
- Tab
- Semicolon

The recommended practice is to use the pipe character ("|") as the delimiter. Use of the comma delimiter is discouraged because commas are often included in data fields as part of the data. For example, a street address might contain a comma.

# Selecting the CSV file character set

You must specify the character set for the CSV file. The default is UTF-8.

All supported character sets are listed in the drop-down menu.

# Mapping attributes and parameter keys to CSV fields

To configure the CSV Lookup Plug-In, you enter the execution code in the Attribute Mapping field. This code maps the lookup parameter keys and custom attributes to column headers in the CSV file. One or more attribute=column pairs is used to map the incident attributes to the column heads. The keys property in the attribute map identifies which columns to use for the lookup.

Here is an example CSV file attribute mapping:

```
attr.Store-ID=store-id
attr.Store\ Address=store address
attr.incident-id=incident-id-key
attr.sender-email=sender-email-key
keys=sender-email-key:incident-id-key
```

With this example in mind, adhere to the following syntactical rules when mapping the attributes to CSV file data.

Table 50-19 Attribute mapping syntax for CSV files

Example and syntax	Description
attr.Store-ID=store-id	Attributes map to column header names in attribute-column pairs.
attr.attribute_name=column_head	Here, <b>Store-ID</b> is a custom attribute and <b>store-id</b> is a column header name in the CSV file.
attr.Store\ Address=store_address	Spaces are allowed before and after the = sign (except for the LDAP Lookup Plugin).
attr.attribute\ name=column\ head	Blank spaces in attribute and column names must be preceded by a backslash.
	Here, the custom attribute is named <b>Store Address</b> .

Table 50-19	Attribute r	napping synta	x for CSV files	(continued)
-------------	-------------	---------------	-----------------	-------------

Example and syntax	Description
attr.Store-ID=store-id attr.Store\ Address=store_address attr.attribute_name=column_head attr.attribute_name=column_head	Each attribute-column pair is entered on a separate line.
attr.Store\ Address=STORE_ADDRESS	All syntax is case sensitive.  The identifier attr. must be lower case.  Incident attributes must match the system-definition string precisely.
attr.incident-id=incident-id-key attr.sender-email=sender-email-key attr.attribute_name=column_head	System attributes are mapped to column header names. The column name does not have to match the system attribute, nor does it require the word "key".
<pre>keys=sender-email-key:incident-id-key keys=<column_name_1st>:column_name_2nd</column_name_1st></pre>	Keys map the column name headers to the incident attribute keys you want to use to look up the attribute values. The keys map to the column header names, not to the incident attribute names. The order of appearance determines priority. Once the first incident is located in the CSV file, the other attributes are populated.

# CSV attribute mapping example

Consider another mapping example for the CSV Lookup Plug-In .

```
attr.sender-email = Email
attr.endpoint-user-name = Username
attr.file-owner = File-owner
attr.sender-ip = IP
attr.First\ Name = FIRST_NAME
attr.Last\ Name = LAST_NAME
attr.Business\ Unit = Org
attr.Manager\ Email = Mgr email
attr.Employee\ ID = EMPLOYEE NUMBER
attr.Phone \ Number = Phone
attr.Manager\ Last\ Name = Mgr_lastname
```

```
attr.Manager\ First\ Name = Mgr firstname
attr.Employee\ Email = Emp email
keys = Email:Username:File-owner:IP
```

#### Note the following about this example:

- The first four lines map lookup parameters to column headers.
- The remaining nine lines map custom attributes to column headers.
- A backslash is prepended before each instance of a white-space character in a attribute or column name. In this example, attr.Employee\ Email = Emp email maps the Employee Email custom attribute to the emp email column head.
- The keys property identifies and sequences the keys that are used to extract custom attribute data. Each key is separated with a colon. The order in which you list the keys determines the search sequence. In this example (keys = Email: Username: File-owner: IP), the plug-in first searches the Email column for a value that matches the lookup parameter value of the sender-email which has been passed to the plug-in. If no matching value is found, the plug-in then searches the Username column for a value that matches the endpoint-user-name lookup parameter. If no matching value is found in that column, it then goes on to search the next key (File-owner), and so on.
- The plug-in stops searching after it finds the first matching parameter key-value pair. As a result, the order in which you list the keys column heads is significant.

# Testing and troubleshooting the CSV Lookup Plug-In

If the plug-in does not load, or if the plug-in loads but fails to populate the custom attributes with looked up values, troubleshoot as follows:

#### To test and troubleshoot the CSV Lookup Plug-In

- Verify that the CSV file conforms to the requirements. If more than 10% of the rows in the CSV file violate any of the CSV file requirements, the lookup plug-in does not load.
  - See "Requirements for creating the CSV file" on page 1114.
- 2 Verify that the delimiter you selected is the one used in the CSV file. Note that the system defaults to comma, whereas the recommendation is pipe.
  - See "Choosing the CSV file delimiter" on page 1115.
- Check the attribute mapping. There is no system-provided validation for the attribute map. Make sure that your attribute map adheres to the syntax.

Common syntactical errors include:

- Every entry in the attribute mapping field is case sensitive.
- Spaces in attribute and column names must be identified by a backslash.
- For every attribute=column pair, the data to the right of the equals sign (=) must be a column head name.
- Keys are column header names, not incident attributes.
- If the plug-in fails to load, or the plug-in fails to return looked up values, check the file \SymantecDLP\Protect\logs\tomcat\localhost.<latest-date>.log.
  - Check that the database and table are created and that the CSV file is loaded into the table. To verify, look for lines similar to the following:

```
INFO [com.vontu.lookup.csv.CsvLookup]
creating database
create table using SQL
importing data from file into table LOOKUP having columns
```

**Note:** To process large files, the CSV Lookup Plug-In uses an in-memory database (Apache Derby). Only one instance of Derby can be running per Enforce Server. If a previous instance is running, the CSV Lookup Plug-In does not load. If the database and table are not created, restart the Vontu Manager service and reload the plug-in.

5 If the plug-in fails to return looked up values, check the file \SymantecDLP\Protect\logs\tomcat\localhost.<latest-date>.log.

Look for a warning message indicating that "SQL guery did not return any results." In this case, make sure that the attribute mapping matches the CSV column heads and reload the plug-in if changes were made.

See "Troubleshooting lookup plug-ins" on page 1109.

# CSV Lookup Plug-In tutorial

This tutorial provides instructions for implementing a simple CSV Lookup Plug-In. The purpose of this tutorial is to introduce you to the lookup plug-in feature from a hands-on approach. If you have experience generating incidents, creating custom attributes, and implementing lookup plug-ins this tutorial may be too basic.

See "About the CSV Lookup Plug-In" on page 1094.

#### To implement a simple CSV Lookup Plug-In

- Create the following custom attributes at System > Attributes > Custom Attributes:
  - Manager
  - Deparment
  - Email Address
- 2 Create a pipe delimited CSV file containing the following data.

SENDER | MGR | DEPT | EMAIL

emp@company.com|Merle Manager|Engineering|rmanager@company.com

3 Save the CSV file to the same volume drive where the Enforce Server is installed.

#### For example:

C:\SymantecDLP\Protect\plugins\lookup\csv lookup file.csv.

Create a basic keyword policy.

See "Configuring policies" on page 326.

5 Generate an email incident.

> To trigger the lookup for this example, the incident should be an SMTP incident with the sender of the email being the address emp@company.com. Change the value of sender in the CSV to match the actual value of the email sender.

- 6 Create a new CSV Lookup Plug-In at System > Incident Data > Lookup Plugins > New Plugin.
- Configure the lookup plug-in as follows: 7
  - Name: CSV Lookp Plug-in
  - Description: Look up manager of email sender from CSV file.
  - CSV File Path: C:\SymantecDLP\Protect\plugins\lookup\csv lookup file.csv
  - Delimiter: Pipe []
  - File Encoding: UTF-8
  - Attribute Mapping

Map the system-defined attributes, custom attributes, and lookup parameter keys on separate lines as follows:

attr.sender-email=SENDER attr.Manager=MGR attr.Department=DEPT attr.Email\ Address=EMAIL kevs=SENDER

attr.sender-email = SENDER This is a lookup parameter key from the **Sender** group. It is mapped to

the corresponding column header in the CSV file.

This is a custom attribute defined in Step 1. It is mapped to the attr.Manager = MGR

corresponding column header in the CSV file.

attr.Department = DEPT This is a custom attribute defined in Step 1. It is mapped to the

corresponding column header in the CSV file.

attr.Email \ Address = EMAIL This is a space delimited custom attribute defines in Step 1. It is mapped

to the corresponding column head in the CSV file.

keys = SENDER This line declares one key to perform the lookup. The lookup ceases

once the first key is located, and the attribute values are populated.

8 Save the plug-in configuration.

Select System > Lookup Plugins > Lookup Parameters and select the following lookup parameter key group:

Sender This group contains the sender-email key.

- 10 Select System > Lookup Plugins > Modify Plugin Chain and enable the plug-in.
- 11 Open the **Incident Snapshot** for the incident generated in the Step 4.
- 12 Verify that the unpopulated custom attributes you created in Step 1 appear in the **Attributes** pane to the right of the screen.

If they do not, complete Step 1.

13 Verify that the "Lookup" button appears in the **Attributes** pane above the custom attributes.

If it does not, verify that the **Lookup Attributes** privilege is granted to the user.

Click Reload Plugin after making any changes.

14 Click the Lookup button.

The custom attributes should be populated with values looked up and retrieved from the CSV file.

15 Troubleshoot the plug-in as necessary.

See "Testing and troubleshooting the CSV Lookup Plug-In" on page 1118.

# **Configuring LDAP Lookup Plug-Ins**

To configure one or more LDAP Lookup Plug-ins, complete these tasks.

Table 50-20 Configuring LDAP Lookup Plug-ins

Step	Action	Description
1	Create custom attributes.	See "Configuring custom attributes" on page 1079.
2	Configure a connection to the LDAP server.	A functioning connection to an LDAP server must be available.  See "Requirements for LDAP server connections" on page 1123.  The connection to the LDAP server can be configured from the link in the LDAP Lookup Plug-In .  See "Configuring directory server connections" on page 127.
3	Create a new LDAP Lookup Plug-In .	See "Creating new lookup plug-ins" on page 1102.
4	Map the attributes.	Map the attributes to the corresponding LDAP directory fields. The syntax is as follows:  attr.CustomAttributeName = search_base:   (search_filter=\$variable\$):   ldapAttribute  See "Mapping attributes to LDAP data" on page 1123.  See "Attribute mapping examples for LDAP" on page 1124.
5	Save and enable the plug-in.	The LDAP Lookup Plug-In must be enabled on the Enforce Server.  See "Enabling lookup plug-ins" on page 1107.
6	Test and troubleshoot the LDAP Lookup Plug-In .	See "Troubleshooting lookup plug-ins" on page 1109.

# Requirements for LDAP server connections

The following conditions must be met for Symantec Data Loss Prevention to establish a connection with an LDAP directory:

- The LDAP directory must be running on a host that is accessible to the Enforce Server.
- There must be an LDAP account that the Symantec Data Loss Prevention can use. This account must have read-only access. You must know the user name and password of the account.
- You must know the Fully Qualified Domain Name (FQN) of the LDAP server (the IP address cannot be used).
- You must know the port on the LDAP server which the Enforce Server uses to communicate with the LDAP server. The default is 389.

You can use an LDAP lookup tool such as Softerra LDAP Browser to confirm that you have the correct credentials to connect to the LDAP server. Also confirm that you have the right fields defined to populate your custom attributes.

See "About LDAP Lookup Plug-Ins" on page 1094.

# Mapping attributes to LDAP data

You map system and custom attributes to LDAP data in the **Attribute Mapping** field. Each mapping is entered on a separate line. The order in which these mapping entries appear does not matter.

The attribute mapping syntax for LDAP Lookup Plug-ins is as follows:

```
attr.CustomAttributeName = search base:
  (search filter=$variable$):
  ldapAttribute
```

The following table describes this syntax in more detail.

Table 50-21 LDAP mapping syntax details

Element	Description
CustomAttributeName	The name of the custom attribute as it is defined in the Enforce Server.
	Note: If the name of the attribute contains white-space characters, you must precede each instance of the white space with a backslash. A white-space character is a space or a tab. For example, you need to enter the Business Unit custom attribute as: attr.Business\ Unit
	See "Configuring custom attributes" on page 1079.

Element	Description
search_base	Identifies the LDAP directory.
search_filter	The name of the LDAP attribute (field) that corresponds to the lookup parameter (or other variable) passed to the plug-in from the Enforce Server.
variable	The name of the lookup parameter that contains the value to be used as a key to locate the correct data in the LDAP directory.
	In cases where multiple plug-ins are chained together, the parameter might be a variable that is passed to the LDAP Lookup Plug-In by a previous plug-in.
IdapAttribute	The LDAP attribute whose data value is returned to the Enforce Server. This value is used to populate the custom attribute that is specified in the first element of the entry.

Table 50-21 LDAP mapping syntax details (continued)

See "About LDAP Lookup Plug-Ins" on page 1094.

# Attribute mapping examples for LDAP

The following mappings provide additional attribute mapping examples for LDAP Lookup Plug-ins.

The following example attribute mapping searches the hr.corp LDAP directory for a record with an attribute for mail whose value matches the value of the sender-email lookup parameter. It returns to the Enforce Server the value of the givenName attribute for that record.

```
attr.First\ Name = dc=corp,dc=hr: (mail=$sender-email$):givenName
```

In the following attribute mapping example, a separate line is entered for each custom attribute that is to be populated. In addition, note the use of the TempDeptCode temporary variable. The department code is needed to obtain the department name from the LDAP hierarchy. But only the department name needs to be stored as a custom attribute. The TempDeptCode variable is created for this purpose.

```
attr.First\ Name = cn=users:(mail=$sender-email$):firstName
attr.Last\ Name = cn=users:(mail=$sender-email$):lastName
attr.TempDeptCode = cn=users:(mail=$sender-email$):deptCode
attr.Department = cn=departments:(deptCode=$TempDeptCode$):name
attr.Manager = cn=users:(mail=$sender-email$):manager
```

# Testing and troubleshooting LDAP Lookup Plug-ins

Complete these steps to troubleshoot LDAP Lookup Plug-In implementations.

See "About LDAP Lookup Plug-Ins" on page 1094.

#### To troubleshoot an LDAP Lookup plug-in

If the plug-in does not save correctly, verify the configuration.

Before using the LDAP Lookup Plug-In you should test the connection to the LDAP server. You can use a lookup tool such as the Softerra LDAP Browser to help confirm that you have the correct fields defined.

See "Configuring directory server connections" on page 127.

- 2 Make sure that the plug-in is enabled.
- 3 Make sure that you created the Custom Attribute definitions. In particular, check the attribute mapping. The attribute names must be identical.
- If you made changes, or edited the lookup parameter keys, reload the plug-in. See "Reloading lookup plug-ins" on page 1108.
- 5 Select **Incidents > All Incidents** for the detection server you are using to detect the incident.
- Select (check) several incidents and select **Lookup Attributes** from the Incident Actions drop-down menu. (This action looks up attribute values for all incidents for that form of detection.
- 7 Check the **Incident Snapshot** screen for an incident. Verify that the **Lookup** Custom Attributes are filled with entries retrieved from the LDAP lookup.
- If the correct values are not populated, or there is no value in a custom attribute you have defined, make sure that there are no connection errors are recorded in the Incident History tab.
- Check the Tomcat log file.

See "Troubleshooting lookup plug-ins" on page 1109.

# LDAP Lookup Plug-In tutorial

This tutorial provides steps for implementing a simple LDAP Lookup Plug-In .

#### To implement an LDAP Lookup Plug-In

Create the following custom attributes at **System > Attributes > Custom** Attributes:

#### LDAP givenName

#### LDAP telephoneNumber

2 Create a directory connection for the Active Directory server at System > **Settings > Directory Connections.** 

For example:

Hostname: enforce.dlp.company.com

Port: 389

■ Base DN: dc=enforce,dc=dlp,dc=com

Encryption: None

Authentication: Authenticated

username: userName

password: password

- Test the connection. The system indicates if the connection is successful.
- Create a new LDAP plug-in at System > Lookup Plugins > New Plugin > LDAP.

Name: LDAP Lookup Plug-in

Description: Description for the LDAP Plug-in.

- Select the directory connection created in Step 2.
- Map the attributes to LDAP metadata.

```
attr.LDAP\ givenName = cn=users:(|(givenName=$endpoint-user-name$)(mail=$sender-email$)
(streetAddress=$discoverserver$)):givenName
attr.LDAP\ telephoneNumber = cn=users:(|(givenName=$endpoint-user-name$)(mail=$sender-email$)
(streetAddress=$discoverserver$)):telephoneNumber
```

- Save the plug-in. Verify that the correct save message for the plug-in is displayed.
- Enable the following keys at the **System > Lookup Plugins > Lookup** Parameters page.
  - Incident

- Message
- Sender
- 9 Create an incident that generates one of the lookup parameters. For example, an email incident exposes the sender-email attribute. There must be some corresponding information in the Active Directory server.
- 10 Open the **Incident Snapshot** for the incident.
- 11 Click the Lookup button and verify the custom attributes created in the Step 1 are populated in the right panel.

# **Configuring Script Lookup Plug-Ins**

Complete these steps to implement one or more Script Lookup Plug-Ins to look up external information.

See "Writing scripts for Script Lookup Plug-Ins" on page 1128.

**Table 50-22** Configuring a Script Lookup Plug-In

Step	Action	Description
1	Create custom attributes.	See "Configuring custom attributes" on page 1079.
2	Create the script.	See "Writing scripts for Script Lookup Plug-Ins" on page 1128.
3	Define the Lookup Parameter Keys.	Select the keys to use to extract custom attribute data.  See "Selecting lookup parameters" on page 1102.
4	Create a new Script Plugin.	See "Creating new lookup plug-ins" on page 1102.
5	Enter the Script Command.	This value is the local path to the script engine executable on the Enforce Server host.  See "Specifying the Script Command" on page 1129.
6	Specify the <b>Arguments</b> .	This value is the path to the Python script file to use for attribute lookup and any command line arguments. Begin the script path with the -u argument to improve lookup performance.  See "Specifying the Arguments" on page 1130.
7	Enable the <b>stdin</b> and <b>stout</b> options.	Enable both options to help prevent script injection attacks.  See "Enabling the stdin and stdout options" on page 1130.

Step	Action	Description
8	Optionally, enable protocol filtering.	You can specify the incident types by protocol for passing attribute values to look up scripts.
		See "Enabling incident protocol filtering for scripts" on page 1131.
9	Optionally, enable and encrypt <b>credentials</b> .	You can encrypt and pass credentials required by the script to connect to external systems.
		See "Enabling and encrypting script credentials" on page 1132.
9	Save the plugin.	Verify that the correct save message for the plugin is displayed.
		See "Creating new lookup plug-ins" on page 1102.
10	Enable the lookup plugin.	You can chain scripts together and chain scripts with other lookup plugins.
11	Test the lookup plugin.	Test the lookup plugin.
		See "Troubleshooting lookup plug-ins" on page 1109.

Table 50-22 Configuring a Script Lookup Plug-In (continued)

# Writing scripts for Script Lookup Plug-Ins

If you are using the Script Lookup Plug-In, you must write a script to extract data and populate the custom attributes of each incident. The Script Lookup Plug-In passes attributes to scripts as key-value pairs. In return, scripts must output a set of key-value pairs to standard out (stdout). The plugin uses these key-value pairs to populate custom attributes.

When writing scripts for use with the Script Lookup Plug-In, adhere to the following syntax requirements and calling conventions, including how a script plugin passes arguments to scripts and the required format for script output.

Table 50-23 Script plugin calling conventions

Convention	Syntax	Description
Input	attribute_name=attribute_value	The Script Lookup Plug-In passes attributes to scripts as command-line parameters in the form key=value.

Convention	Syntax	Description
Output	stdout	To work with the plugin and populate attributes, scripts must output a set of key-value pairs to standard out (stdout).
		Newline characters must separate output key-value pairs. For example:
		host-name=mycomputer.company.corp username=DOMAIN\bsmith
exit code	0	Scripts must exit with an exit code of '0.' If scripts exit with any other code, the Enforce Server assumes that an error has occurred in script execution and terminates the attribute lookup.
error handling	stderr to a file	Scripts cannot print out error or debug information. Redirect stderr to a file. In Python this would be:
		<pre>fsock = open("C:\error.log", "a") sys.stde</pre>

Table 50-23 Script plugin calling conventions (continued)

See "Example script" on page 1136.

# Specifying the Script Command

The **Script Command** field specifies the path to the script engine for executing the script. These instructions are specific to Python.

#### To specify the script command

- Download and install version 2.6 of Python on the Enforce Server host, if you have not already done so.
- 2 Enter the local path to the python.exe executable file.

#### For example:

- Windows: c:\python26\python.exe
- Linux: /usr/local/bin/python
- 3 Enter the **Arguments**.

See "Specifying the Arguments" on page 1130.

# Specifying the Arguments

The Arugments field specifies the path to the script and any additional command line arguments. These instructions are specific to Python.

#### To specify the Arguments

- After writing a script, copy it to the Enforce Server host, or to a file share that is accessible by the Enforce Server.
- 2 Make sure that permissions are set correctly on the directory and the script file.

Both the directory and file must be readable and executable by the protect user.

3 Enter the -u argument in the **Argument** field.

This command forces stdin, stdout, and stderr to be totally unbuffered, which improves lookup performance.

Enter the fully qualified path to the script file.

For example:

- Windows: -u, c:\python26\scripts\ip-lookup.py
- Linux: -u, /opt/python26/scripts/ip-lookup.py

Note: The system does not validate the file location.

5 Save the plugin configuration.

# Enabling the stdin and stdout options

When you configure a Script Lookup Plug-In you can choose to Enable stdin and Enable stdout. If these options are enabled, the system checks the script input and output for unsafe characters such as command delimiters and logical operators that could be exploited by a UNIX or Windows shell.

Because you are running the script on the host where the Enforcer Server is installed, you should enable both options, unless you are certain that your script is safe. If enabled, the logs will indicate invalid and unescaped characters.

See Table 50-24 on page 1131.

Table 50-24 Invalid characters for attribute names

Invalid character	Description
Empty string	Empty strings are not allowed.
@	Attributes containing these characters will be ignored during processing if the stdin and stdout options are enabled.
+	
=	
:	
/	
\	
)	
(	
-	
+	
_	
\$	Attributes containing the \$ and % characters are allowed if these characters are properly
8	escaped by a backslash.

# Enabling incident protocol filtering for scripts

Optionally, you can specify the incident types (by protocol) for passing attribute values to look up scripts. If you do not enable protocol filtering, your Script Lookup Plug-In will apply to all incidents.

For example, you can limit the passing of attribute values to those incidents that are detected over HTTP. When you filter by protocol, Enforce Server still captures the incidents that are detected over other protocols. But it does not use the Script Lookup Plug-In to populate those incidents with attribute values.

#### To enable protocol filtering

- Navigate to the System > Lookup Plugins > Edit Script Lookup Plugin screen in the Enforce Server administration console.
  - See "Configuring Script Lookup Plug-Ins" on page 1127.
- 2 At the Script Lookup Plugin screen, select (check) the Enable protocol filtering option.

This action displays all the protocols that are available for filtering. Note that protocols are detection server-specific.

Note: Network and Mobile protocols are configured at the System > Settings > Protocols screen. Endpoint protocols are configured at the System > Agents > Agent Configuration screen. Discover protocols are configured at the Policies > Discover Scanning > Discover Targets. And, once an incident is generated, the protocol value for the incident is displayed at the top of the Incident Snapshot screen.

- 3 Specify the protocols you want to include in the lookup. If you enable protocol filtering, you must select at least one protocol on which to filter.
- Save the plug-in configuration.

# Enabling and encrypting script credentials

If your script is connecting to an external system that requires credentials, you can enable credentials for your script. If you enable credentials through the user interface option, you must encrypt them. Symantec Data Loss Prevention provides the Credential Utility, which lets you encrypt credentials and use them to authenticate to an external data source.

When the Enforce Server invokes the Script Lookup Plug-In, the plug-in decrypts any credentials at runtime and passes them to the script as attributes. The credentials are then available for use within the script. The Credential Utility uses the same platform encryption keys that are used to protect user accounts and incident information within the Symantec Data Loss Prevention system.

See Table 50-25 on page 1133.

If you choose to use credentials in clear text, you must hard code them into your script. In this case, the Enforce Server passes the values you exported to the clear-text credential file. These values are passed in the following format: key=value.

Enabling and encrypting credentials Table 50-25

Step	Action	Description
1	Create a text file that contains the	The format of this file is $key=value$ , where $key$ is the name
	credentials that are needed by the script to access the appropriate external	
	systems.	For example:
		username=msantos password=esperanza9
2	Save this credential file to the file system	The file needs to be saved to the Enforce Server temporarily.
	local to the Enforce Server.	For example: C:\temp\MyCredentials.txt.
3	On the Enforce Server, open a shell or command prompt and change directories to \SymantecDLP_home\Protect\bin.	This directory on the Enforce Server contains the Credential Generator Utility.
4	Issue a command to generate an	The command syntax is as follows:
	encrypted credential file.	CredentialGenerator.bat
		in-cleartext-filepath out-encrypted-filepath
		For example on Windows you would issue the following:
		CredentialGenerator.bat C:\temp\MyCredentials. C:\temp\MyCredentialsEncrypted.txt
		You can open this file in a text editor to verify that it is encrypted.
5	Select Enable Credentials.	At the System > Lookup Plugins > Edit Script Lookup Plugin page, select (check) the Enable Credentials option.
6	Enter the Credentials File Path.	Enter the fully qualified path to the encrypted credentials file. For example:
		C:\temp\MyCredentialsEncrypted.txt.
7	Save the plug-in.	You can now use the encrypted credentials to authenticate to an external system.
8	Secure the clear-text credentials file.	If you want to save the clear-text credentials file, move it to a secure location. It can be useful to save the file if you plan to update and re-encrypt it later. If you do not want to save the file, delete it now.
9	Reload the lookup plug-in.	See "Managing and configuring lookup plug-ins" on page 1100.

# Chaining multiple Script Lookup Plug-Ins

All lookup plug-ins receive a reference to the same attribute map. This reference enables you to chain lookup plug-ins. Whether plug-in chaining is necessary to populate your custom attributes varies according to circumstances. Consider the following example scenarios.

Getting the right key for Network email incidents is usually straightforward. The email address of the message sender is automatically captured as the sender-email lookup parameter. That lookup parameter can be used as a key to unlock the information about the sender that is stored in an external source. In this instance, it is not necessary to chain multiple plug-ins.

For Web or FTP incidents, a plug-in chain might be necessary. The lookup parameter that is captured for these kinds of incidents is the IP addresses of the originating hosts. But IP addresses usually are not static identifiers like email addresses. Therefore, you may need to do successive lookups to get to a static identifier that can be used as an information key.

You can write a script to pass the sender-ip lookup parameter to a DNS server to get the host name. You can then write another script to pass that host name to an asset management system. From the asset management system you can obtain the user name or email of the person using that computer. That user name or email can then be used as the "key" to unlock the rest of the data. This plug-in chain would have three links:

- 1. The Script Lookup Plug-In that uses the IP address to return the host name.
- 2. The Script Lookup Plug-In that uses the host name to return the user name or email.
- 3. The CSV Lookup Plug-In that uses the user name or email to return the rest of the custom attribute data.

In this example, you must create a new Host Name temporary variable to store the host name information. This temporary variable and its value are then available to the second script and subsequent plugins.

# Script Lookup Plug-In tutorial

Complete the following tutorial to implement a Script Lookup Plug-In . This tutorial assumes basic hands-on familiarity with implementing lookup plugins. To obtain this familiarity, complete the "CSV Lookup Plug-In tutorial."

See "CSV Lookup Plug-In tutorial" on page 1119.

#### To implement a Script Lookup Plug-In

1 Download and install Python 2.6 on the system where the Enforce Server is installed.

For example: C:\python26.

2 Copy the "Example script" provided in this chapter to a text file and save it to a directory on the Enforce Server host as Script-Plug-In.py.

For example: C:\python26\scripts\Script-Plug-In.py.

See "Example script" on page 1136.

- Open this script in a Python IDE such as the Wing IDE (available at http://www.wingware.com/).
- 4 Review the comments in this script and run it.
  - Comment out line 18.
  - Run the script. It returns "Script-attribute=script value".
  - Uncomment line 18 so it is not processed.
- 5 Create the following custom attribute: Script-attribute.
- Select New Plugin > Script to create a new Script Lookup Plug-In . 6

See "Creating new lookup plug-ins" on page 1102.

7 Configure the Script Lookup Plug-In.

Use the following parameters:

- Script Command: C:\python26\python.exe
- **Arguments**: -u, C:\python26\scripts\Script-Plugin.py
- Save the plugin and ensure that the plugin loads successfully as indicated by the system message.
- Enable the following lookup parameters: **Incident**, **Message**, and **Sender**.
- 10 Generate an incident that passes the date-sent attribute.
- 11 Go to the Incident Snapshot for the new incident and click **Lookup**.
- 12 Verify that the Script-attribute custom attribute is populated with the value of script value.

13 If the custom attribute is not populated, check the log file

C:\SymantecDLP\Protect\logs\tomcat\localhost.<latest date>.log.

If Script-attribute=null check the script. Review the comments in the provided script and ensure that there is no space between the attribute=value pair.

See "Troubleshooting lookup plug-ins" on page 1109.

14 Explore enabling optional properties for the Script Lookup Plug-In, including stdin/stdout, protocol filtering, and credentials.

See "Enabling the stdin and stdout options" on page 1130.

See "Enabling incident protocol filtering for scripts" on page 1131.

See "Chaining multiple Script Lookup Plug-Ins" on page 1134.

# Example script

The following script is provided as an example for the Script Lookup Plug-In . It is written in Python 2.6. The purpose of this script is to provide a basic working example for writing scripts in Python that can be used for Script Lookup Plugins.

This script contains the date-sent lookup parameter key and returns the "script value" for the custom attribute Script-attribute.

See "Script Lookup Plug-In tutorial" on page 1134.

Note: Because Python is strict about indentation requirements, if you copy/paste this example script you will likely need to reformat it so that it appears exactly as displayed here.

```
name =" main "
import sys, os, traceback
import commands
# Switch this to 0 when in production mode.
debugMode = 1
def main(args):
    try:
        attributeMap = parseInput(args)
        # This is the lookup parameter key.
        # Comment-out this line for testing the script standalone.
        dateSent = attributeMap["date-sent"]
        # "Script-attribute" is the custom attribute.
        # "script value" is the return value.
        # You cannot have a space between the custom attribute and the
        # attribute value. For example, "Script-attribute = script value"
        # Does not work for Script Lookup Plugins.
        print "Script-attribute=script value"
        return
    except:
        error()
        print "something went wrong!"
        return "something went wrong!"
def parseInput(args):
    # Input data is a list of key value pairs seperated by carraige return
    # Create a python dictionary to create the attribute map
    attributeMap = {}
   delimiter = "="
    for item in args:
        if delimiter in item:
            tuple = item.split(delimiter)
            attributeMap[tuple[0]] = tuple[1]
    return attributeMap
def error():
    # "SCRIPT PROCESSING ERROR"
    if (debugMode):
```

```
#print "Script Processing Error"
        traceback.print exc(file=sys.stdout)
    return ""
# DOS-style shells (for DOS, NT, OS/2):
def getstatusoutput(cmd):
    """ Return (status, output) of executing cmd in a
   shell."""
   pipe = os.popen(cmd + ' 2>&1', 'r')
   text = pipe.read()
   sts = pipe.close()
   if sts is None: sts = 0
   if text[-1:] == '\n': text = text[:-1]
   return sts, text
# Entry Point
if name == " main ":
      if(len(sys.argv) == 0):
          error()
      else:
          main(sys.argv)
```

# Configuring migrated Custom (Legacy) Lookup Plug-Ins

These steps presume that you have existing Custom Java Lookup Plug-Ins deployed to a pre-12.0 version of Symantec Data Loss Prevention and that you have upgraded the system to Symantec Data Loss Prevention version 12.0 or later. In this case a Custom Java Lookup Plug-In will be migrated to a Custom (Legacy) Lookup Plug-In and will appear in the user interface for verification and testing.

See "About Custom (Legacy) Lookup Plug-Ins" on page 1095.

#### Implementing Custom (Legacy) Lookup Plugins Table 50-26

Step	Action	Description
1	Create custom attributes.	Create the custom attributes that your Custom (Legacy) Lookup Plugin will retrieve the values for.
		See "About using custom attributes" on page 1078.
2	Edit the Custom (Legacy) Plugin.	Successful upgrade should import the Custom (Legacy) Lookup Plugin to the user interface where you can enable it.
		You can update the name and description if necessary.
		See "Creating new lookup plug-ins" on page 1102.
3	Verify the <b>Plugin Class</b> .	After upgrade, the class name should be populated from the Plugins.properties file.
4	Verify the <b>Required JARs</b> .	After upgrade, the JAR files previously copied to the Enforce Server should appear in this field.
5	Enable the plug-in.	Turn the plug-in <b>On</b> .
		See "Enabling lookup plug-ins" on page 1107.
6	Enable parameter lookup keys.	Select the keys to trigger attribute lookup.
		See "Selecting lookup parameters" on page 1102.
7	Create a policy and generate an incident of the type expected by the plug-in.	For example, create a keyword policy and generate an SMTP network incident that passes the sender-name attribute.
8	Verify that the custom attributes are updated.	Check the <b>Incident Snapshot</b> for the populated attributes.  See "Troubleshooting lookup plug-ins" on page 1109.

Section

# Monitoring and preventing data loss in the network

- Chapter 51. Implementing Network Monitor
- Chapter 52. Implementing Network Prevent for Email
- Chapter 53. Implementing Network Prevent for Web

# Implementing Network Monitor

This chapter includes the following topics:

- Implementing Network Monitor
- About IPv6 support for Network Monitor
- Choosing a network packet capture method
- About packet capture software installation and configuration
- Configuring the Network Monitor Server
- Enabling GET processing with Network Monitor
- Creating a policy for Network Monitor
- Testing Network Monitor

# Implementing Network Monitor

Network Monitor captures and analyzes traffic on your network, detecting confidential data, and significant traffic metadata over protocols you specify. For example, SMTP, FTP, HTTP, and various IM protocols. You can configure a Network Monitor Server to monitor custom protocols and to use a variety of filters (per protocol) to filter out low-risk traffic.

To monitor network traffic, a Network Monitor Server requires:

 A network Switch Port Analyzer (SPAN) or network tap to acquire traffic on the target network.

- A card on the Network Monitor Server host to capture the network traffic that is acquired from the SPAN or tap. Either a network interface card (NIC) or high-speed packet capture adapter (Endace or Napatech) can be used. (Note that in addition to this traffic-capturing card, a separate NIC is required for communication between the Network Monitor Server and the Enforce Server. WinPcap is required for this purpose.)
- Packet capture software. When you use a NIC for packet capture, packet capture software must be installed on the Network Monitor Server host. When you use a high-speed packet capture adapter card (Endace or Napatech), the card must use the correct driver.

See "Choosing a network packet capture method" on page 1144.

Secured Corporate LAN DMZ Chat Email Web Other Internet IREWALL Span/Tap Corporate User Port Secure Encrypted Channel Administrator Created Deployed Network Enforce Monitor

Figure 51-1 A basic Network Monitor setup

To implement packet capture and set up a Network Monitor, perform the following high-level tasks:

- 1 Install and set up the network tap or SPAN that captures network traffic.
- 2 Choose a method of capturing network traffic. See "Choosing a network packet capture method" on page 1144.
- 3 Install the necessary NIC or high-speed packet capture adapter (Endace or Napatech) on the Network Monitor as described by the card documentation. Also use the appropriate Symantec Data Loss Prevention Installation Guide (Windows or Linux). This NIC or high-speed packet capture adapter (Endace or Napatech) must operate in promiscuous mode so that all inbound and outbound traffic is relayed through this port.
  - See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about supported NICs and high-speed packet capture adapters.

- On a Windows platform, install WinPcap if it is not already installed.
  - See "Installing WinPcap on a Windows platform" on page 1146.
- 5 If necessary, update the driver for the high-speed packet capture adapter.
  - See "Updating the Endace card driver" on page 1146.
  - See "Installing and updating the Napatech network adapter and driver software" on page 1146.
- Disable checksum offloading for the NIC that is used to monitor network traffic. For Linux platforms, use the following commands to disable checksum offloading for both receiving and transmitted data on the eth0 interface:

```
ethtool -K eth0 tx off
ethtool -K eth0 rx off
```

To see the current status of checksum offloading, use the ethtool -k eth0 command.

Note: Certain checksum algorithms work by modifying network packets and adding empty checksums. Empty checksums can cause network capture drivers to drop the packets, in which case they are not evaluated by Network Monitor.

- Use a protocol analyzer such as Wireshark to validate traffic on the tap or SPAN that feeds into your NIC or high-speed packet capture adapter (Endace or Napatech).
- Configure the Network Monitor Server.
  - See "Configuring the Network Monitor Server" on page 1147.
- Create and deploy a test policy for Network Monitor.
  - See "Creating a policy for Network Monitor" on page 1150.
- 10 Test the system by generating an incident against your test policy.
  - See "Testing Network Monitor" on page 1151.

# About IPv6 support for Network Monitor

Symantec Data Loss Prevention supports monitoring of pure IPv4 networks, dual-stack (IPv4 and IPv6) networks, or pure IPv6 networks. The Enforce Server administration console supports input and reporting of both IPv4 and IPv6 addresses for Network Monitor. Support for monitoring IPv6 networks is limited to

implementations of Network Monitor and does not include support for other Symantec Data Loss Prevention products.

Here is an overview of specific support for IPv6 in Symantec Data Loss Prevention:

- Installation of a Network Monitor Server that is capable of monitoring IPv6 networks or dual-stack networks is the same as installation of a Network Monitor Server that monitors an IPv4 network.
- The hardware and operating system requirements are the same as for IPv4 Network Monitor. See the Symantec Data Loss Prevention System Requirements Guide for more information on third-party hardware and software compatibility.
- IP address data types can hold either IPv4 or IPv6 addresses.
- Network incidents can include IPv6 addresses.
- Network protocol definitions can include IPv6 addresses.

Symantec Data Loss Prevention IPv6 support is limited to monitoring. The Enforce Server administration console must still be deployed on an IPv4 network; there is no support for command and control functionality over IPv6.

This release does not include support for:

- Deployment of Symantec Data Loss Prevention over IPv6 networks
- Support of other Symantec Data Loss Prevention servers on IPv6 networks
- Use of IPv6 system-defined data identifiers
- Use of IP fragmentation over IPv6
- Configuring or communicating with detection servers over IPv6
- Deployment of IPv6 endpoints
- Deployment of Symantec Encryption Server on IPv6
- Deployment of the Oracle database on an IPv6 connection

See Configure a protocol in online Help for more information about specific implementation details of IPv6 support.

# Choosing a network packet capture method

You can use three different methods to capture the network traffic that is acquired by a SPAN or tap:

 NIC on a Windows platform. Windows platforms using a NIC for packet capture require a WinPcap library on the Network Monitor Server host. If WinPcap is not already on the Network Monitor Server host, you must install it. See the

Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about the supported version of the WinPcap library. See "Installing WinPcap on a Windows platform" on page 1146.

- NIC on a Linux platform. Linux platforms using a NIC use native Linux packet capture which requires PACKET MMAP support in the kernel. Support for PACKET MMAP is included by default in supported Linux kernels.
- High-speed packet capture adapter on either Windows or Linux platforms. An Endace DAG network measurement card can be used on Linux 64-bit platforms to provide network packet capture in high-traffic environments. Alternatively, a Napatech network adapter can be used to provide network packet capture. See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about supported high-speed packet capture adapters and drivers.

Table 51-1 Packet capture alternatives

Packet capture type	Platform	Software
NIC	Windows	WinPcap
	Linux	Native
High-speed packet capture adapter	Windows 64-bit	Napatech
	Linux 64-bit	Endace
		Napatech

# About packet capture software installation and configuration

Consider the following requirements when installing and configuring packet capture software:

- On Windows platforms, packet capture requires the WinPcap software which may need to be installed if it is not already present.
- On Linux platforms, PACKET MMAP performs packet capture. PACKET MMAP is a standard Linux component and should not need to be installed or modified. However, you also require apr-util, apr, expat, and other third-party packages to run a Network Monitor Server on Linux. See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for more information.

 If you use a high-speed packet capture adapter (Endace or Napatech), you will need to install or update the adpater driver software.

See "Installing WinPcap on a Windows platform" on page 1146.

See "Updating the Endace card driver" on page 1146.

See "Installing and updating the Napatech network adapter and driver software" on page 1146.

# Installing WinPcap on a Windows platform

If WinPcap software is not already present on a Windows platform, you must install it. See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about the supported version of the WinPcap library. Additional details can be found in the Symantec Data Loss Prevention Installation Guide.

See "About managing Symantec Data Loss Prevention servers" on page 177.

#### To install WinPcap on the Network Monitor detection server:

- Copy the WinPcap files to a local drive.
- 2 Run the WinPcap executable and follow the installation instructions.
- 3 Reset the Windows registry settings by running pcapstart.reg and follow the instructions that are displayed.

# Updating the Endace card driver

If you upgrade a Network Monitor Server to the current version, you may need to update the Endace card driver. See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about supported Endace cards and drivers.

#### **Updating an Endace Driver**

- Install the new driver as described by Endace documentation.
- 2 Reconfigure the Network Monitor to use the new driver. See "Configuring the Network Monitor Server" on page 1147.

### Installing and updating the Napatech network adapter and driver software

This topic provides instructions for installing the Napatech high-speed packet capture adapter. Refer to the Symantec Data Loss Prevention System Requirements and Compatibility Guide for information about the supported Napatech card and driver versions.

Table 51-2 Installing and updating the Napatech network adapter

Step	Action	Description
1	Install the supported Napatech high-speed packet capture adapter.	Refer to the Symantec Data Loss Prevention System Requirements and Compatibility Guide for the supported Napatech card version.
2	Install the Napatech driver.	For supported versions of the Napatech driver, see the Symantec Data Loss Prevention System Requirements and Compatibility Guide.
3	Verify Napatech installation.	For Windows:  Make sure that the Napatech library file <code>CommonLib.dll</code> is present in directory <code>\<windows_installation_drive>\Windows\System32\</windows_installation_drive></code> .  For Linux:  The Napatech driver has to be compiled from source as a part of installing Napatech software package (see step 2 above).  The Napatech driver has to be loaded using the script <code>/opt/napatech/bin/load_driver.sh</code> once for each computer bootstrap before capturing packets. Note for RHEL Linux, edit the file <code>/etc/rc.d/rc.local</code> to append <code>/opt/napatech/bin/load_driver.sh</code> and restart the system.  Verify that the Napatech library file <code>libntcommoninterface.so</code> is present in directory <code>/<nt_installation_directory>/lib/</nt_installation_directory></code> .
4	Configure the Network Monitor detection server.	Deploy a Network Monitor detection server and configure the Advanced Server settings:  ■ Enable Napatech packet capture by setting the following flag to true:  PacketCapture.IS_NAPATECH_ENABLED.  ■ Update the value to the path to the Napatech driver tools directory by entering the path in the field for the following entry: PacketCapture.NAPATECH_TOOLS_PATH.  ■ For example, on Windows Napatech tools binaries are included as part of the Napatech software package:  \timespackage.windows_dersion>\tools\timespackage.sion>\tools\timespackage.indows_dersion>\timespackage.indows_dersio

# **Configuring the Network Monitor Server**

You configure the Network Monitor Server by selecting the network interface (NIC, Napatech, or Endace card) to use for traffic capture. You must also select which protocols to monitor.

#### To configure a Network Monitor Server

In the Enforce Server administration console, go to System > Servers > Overview and click the Network Monitor Server. The Server Detail screen appears.

If you do not use a high-speed packet capture adapter (Endace or Napatech) for traffic capture, skip to step 6.

- 2 If you use a high-speed packet capture adapter (Endace or Napatech), click Server Settings.
- **3** For Endace cards, enter the appropriate values in the following fields:

PacketCapture.ENDACE_BIN_PATH	Type the path to the Endace \bin directory.
	By default, this directory is located at endace_home\dag-version\bin. Note that you cannot use variables (such as %ENDACE_HOME%) in any of the fields that are listed here.
PacketCapture.ENDACE_LIB_PATH	Type the path to the Endace \lib directory
PacketCapture.ENDACE_XILINX_PATH	Type the path to the Endace $\verb \xilinx $ directory.
PacketCapture.IS ENDACE ENABLED	Change the value to true.

4 For Napatech cards, enter the appropriate values in the following fields:

PacketCapture.IS NAPATECH ENABLED Change the value to true. PacketCapture.NAPATECH\_TOOLS\_PATH Type the path to the Napatech \tools directory.

- 5 Stop and restart the Network Monitor Server. Symantec Data Loss Prevention displays the Endace card in the Network Interfaces field of the Configure Server screen for the Network Monitor Server.
- 6 Go to System > Servers > Overview and again click on the Network Monitor Server.
- On the Server Detail screen, click **Configure**. You can verify or modify settings in the general section at top and on the Packet Capture tab, as described in subsequent steps.

- Leave the Source Folder Override field blank to accept the default directory for buffering network streams before the Network Monitor Server processes them. (This setting is the recommended setting.) To specify a custom buffer directory, type the full path to the directory.
- Leave the Archive Folder field blank.
- 10 Select one or more **Network Interfaces** (NICs, Napatech cards, or Endace cards) through which the Network Monitor Server should capture traffic.
- 11 In the **Protocol** section, select one or more protocols to monitor. For example, select the check boxes for SMTP, HTTP, and FTP. For a protocol to appear in this section, it must already be configured on the global Protocols screen in the Enforce Server.
  - See the online Help associated with the **Configure Server** screen.
  - Symantec Data Loss Prevention has standard settings for each protocol in the list. To modify a protocol's settings, click the **Pencil** icon next to the appropriate protocol. For details on modifying protocol settings, see the online Help.
- 12 Click Save.
- 13 Stop and restart the Network Monitor Server. Click Recycle next to the Status entry in the Server Detail screen.

After selecting a network interface and choosing protocols, you may want to create a test policy to test your deployment.

See "Testing Network Monitor" on page 1151.

See "Enabling GET processing with Network Monitor" on page 1149.

See "Creating a policy for Network Monitor" on page 1150.

# **Enabling GET processing with Network Monitor**

By default, Network Monitor does not process HTTP GET commands. GET processing is disabled because it involves high traffic volume, and because sensitive data is rarely lost in GET commands. If you require GET processing and the Network Monitor Server can handle the increased load, follow this procedure to configure Network Monitor to process GET commands.

Note: Network Monitoronly inspects GET requests, it does not inspect HTTP GET responses.

#### To enable GET processing

- Ensure that the **L7.processGets** advanced server setting on the Network Monitor Server true (which is the default).
- Change the PacketCapture.DISCARD\_HTTP\_GET advanced server setting on the Network Monitor Server from the default setting of true to false.
- Reduce the size of the L7.minSizeofGetURL advanced server setting on the 3 Network Monitor Server from the default of 100. Reduce it to a number of bytes smaller than the length of the shortest URL from which you want to process GET commands. A minimum URL size of 10 should cover all cases. Note, however, that reducing the minimum size of GETs increases the number of requests that have to be processed, which increases the server's traffic load.

Note: Network Monitoronly inspects HTTP GET requests; it does not inspect HTTP GET responses.

See "Enabling GET processing for Network Prevent for Web" on page 1174.

# Creating a policy for Network Monitor

For Network Monitor, you can create the policies that include any of the standard response rules. To set up a response rule action, go to Manage > Policies > Response Rules and click Add Response Rules.

See "Workflow for implementing policies" on page 293.

#### To create a test policy for Network Monitor

- In the Enforce Server administration console, create a response rule that includes one of the actions that applies to Network Monitor. For example, create a response rule that includes the All: Set Status action.
  - See "Configuring response rules" on page 891.
- 2 Create a policy that incorporates the response rule you configured in the previous step.

For example, create a policy called Test Policy as follows:

- Include a Content Matches Keyword detection rule that matches on the keyword test dlp secret keyword.
- Include an All: Set Status response rule.
- Associate it with the Default policy group.

See "Adding a new policy or policy template" on page 325.

See "Configuring policies" on page 326.

# **Testing Network Monitor**

You can test Network Monitor by sending an email that violates your test policy.

#### To test your system

- Access an email account that routes messages through the MTA.
- Send an email that contains confidential data. For example, send an email that contains the keyword test\_dlp\_secret\_keyword.
- 3 In the Enforce Server administration console, go to Incidents > Network and click Incidents - New. Look for the resulting incident. For example, search for an incident entry that includes the appropriate timestamp and policy name.
- 4 Click on the relevant incident entry to see the complete incident snapshot. See "About Symantec Data Loss Prevention reports" on page 1006.

See "Configuring the Network Monitor Server" on page 1147.

See "Creating a policy for Network Monitor" on page 1150.

# Implementing Network Prevent for Email

This chapter includes the following topics:

- Implementing Network Prevent for Email
- About Mail Transfer Agent (MTA) integration
- Configuring Network Prevent for Email Server for reflecting or forwarding mode
- Specifying one or more upstream mail transfer agents (MTAs)
- Creating a policy for Network Prevent for Email
- About policy violation data headers
- Enabling policy violation data headers
- Testing Network Prevent for Email

# Implementing Network Prevent for Email

Network Prevent for Email monitors and analyzes outbound email traffic in-line and (optionally) blocks, redirects, or modifies email messages as specified in your policies. Network Prevent for Email integrates with industry-standard mail transfer agents (MTAs) and hosted email services to let you monitor and stop data loss incidents over SMTP. Policies that are deployed on the Network Prevent for Email Server direct the Prevent-integrated MTA or hosted email server. The Prevent-integrated mail server blocks, reroutes, and alters email messages based on specific content or other message attributes.

Note: Review the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent for Email to determine your preferred integration architecture before you continue with the implementation.

Figure 52-1 shows an integration of Network Prevent for Email Server with a next-hop MTA that you manage in the network. As an alternative, you can integrate Network Prevent for Email Server with a hosted email server that resides outside the firewall.

Secured Corporate LAN Corporate User Policies Web other Deployed DM7 FTP Mail AV/AS Span/Tap MTA MTA Chat SMTP Email Internet Span/Tap Port Secure, Encrypted Channel Network 4onitor Policies Deployed Enforce Network Prevent Quarantine Encryption for (option) (option) **Email** Administrator Policies Policies Created Deployed

A basic Network Prevent for Email setup Figure 52-1

First, you need to know the high-level steps that are required for implementing Network Prevent for Email. You can check the cross-referenced sections for more details.

#### To implement Network Prevent for Email

- Choose an integration architecture and configure your Mail Transfer Agent (MTA) to work with the Network Prevent for Email Server.
  - See "About Mail Transfer Agent (MTA) integration" on page 1154.
- 2 Configure the Network Prevent for Email Server to work within your chosen integration architecture.
  - See "Configuring Network Prevent for Email Server for reflecting or forwarding mode" on page 1155.
- If you plan to encrypt or quarantine email messages, configure the necessary third-party encryption server(s) or archiving servers. For details, see your product's documentation.
- Create and deploy a policy for Network Prevent for Email.
  - See "Creating a policy for Network Prevent for Email" on page 1161.
- 5 Test the system by generating an incident against your test policy. See "Testing Network Prevent for Email" on page 1164.

## About Mail Transfer Agent (MTA) integration

Choose an integration architecture and configure your Mail Transfer Agent (MTA) to work with the Network Prevent for Email Server.

Review the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent for Email. Familiarize yourself with the compatible integration architectures.

The Network Prevent for Email Server can operate with your MTA in either reflecting or forwarding modes:

- Reflecting mode. In reflecting mode, the Network Prevent for Email Server receives messages from an MTA. It analyzes them, and then returns them to the same MTA (with instructions to block the messages or process them downstream). In essence, the server returns messages to the same IP address from which they arrived.
- Forwarding mode. In forwarding mode, the Network Prevent for Email Server receives messages from an upstream MTA. It analyzes them, and then sends them on to a downstream MTA or hosted email service provider. You can specify a list of IP addresses or hostnames for the next-hop mail server in the Network Prevent for Email Server configuration.

You can also configure a single Network Prevent for Email Server to work with multiple MTAs.

See "Specifying one or more upstream mail transfer agents (MTAs)" on page 1160.

## **Configuring Network Prevent for Email Server for** reflecting or forwarding mode

Use the following instructions to configure Network Prevent for Email Server to operate either in reflecting or forwarding mode.

#### To configure the Network Prevent for Email Server

- Log on to the Enforce Server administration console for the Symantec Data Loss Prevention system you want to configure.
- 2 Select **System > Servers > Overview** to display the list of configured servers.
- Click the name of the Network Prevent for Email Server that you want to configure.
- Click Configure. 4
- 5 Deselect **Trial Mode** to enable blocking of email messages that are found to violate Symantec Data Loss Prevention policies.

successfully configure forwarding mode

6 Configure reflecting mode or forwarding mode by modifying the following fields:

Field	Description
Next Hop Configuration	Select <b>Reflect</b> to operate Network Prevent for Email Server in reflecting mode. Select <b>Forward</b> to operate in forwarding mode.
	<b>Note:</b> If you select <b>Forward</b> you must also select <b>Enable MX Lookup</b> or <b>Disable MX Lookup</b> to configure the method used to determine the next-hop MTA.
Enable MX Lookup	This option applies only to forwarding mode configurations.
	Select <b>Enable MX Lookup</b> to perform a DNS query on a domain name to obtain the mail exchange (MX) records for the server. Network Prevent for Email Server uses the returned MX records to select the address of the next hop mail server.
	If you select <b>Enable MX Lookup</b> , also add one or more domain names in the <b>Enter Domains</b> text box. For example:
	companyname.com
	Network Prevent for Email Server performs MX record queries for the domain names that you specify.
	<b>Note:</b> You must include at least one valid entry in the <b>Enter Domains</b> text box to

behavior.

F	ie	ч	d
			u

#### Disable MX Lookup

#### Description

This field applies only to forwarding mode configurations.

Select **Disable MX Lookup** if you want to specify the exact hostname or IP address of one or more next-hop MTAs. Network Prevent for Email Server uses the hostnames or addresses that you specify and does not perform an MX record lookup.

If you select Disable MX Lookup, also add one or more hostnames or IP addresses for next-hop MTAs in the Enter **Hostnames** text box. You can specify multiple entries by placing each entry on a separate line. For example:

```
smtp1.companyname.com
smtp2.companyname.com
smtp3.companyname.com
```

Network Prevent for Email Server always tries to proxy to the first MTA that you specify in the list. If that MTA is not available, Network Prevent for Email Server tries the next available entry in the list

Note: You must include at least one valid entry in the Enter Hostnames text box to successfully configure forwarding mode behavior.

8 Click **Server Settings** to verify or configure these advanced settings:

Field	Description
RequestProcessor.ServerSocketPort	Ensure that this value matches the number of the SMTP Listener port to which the upstream MTA sends email messages. The default is 10025.
	Note: Many Linux systems restrict ports below 1024 to root access. Network Prevent for Email cannot bind to these restricted ports. If the computer receives mail for inspection on a restricted port (for example, port 25), reconfigure the computer to route traffic from the restricted port to the non-restricted Network Prevent for Email port (port 10025 by default).
	See "Configuring Linux IP tables to reroute traffic from a restricted port" on page 1159.
RequestProcessor.MTAResubmitPort	Ensure that this value matches the number of the SMTP Listener port on the upstream MTA to which the Network Prevent for Email Server returns mail. The default is 10026.
RequestProcessor.AddDefaultHeader	By default, Network Prevent for Email Server uses a header to identify all email messages that it has processed. The header and value are specified in the RequestProcessor.DefaultPassHeader field.
	Change the value of this field to false if you do not want to add a header to each message.

Field	Description
RequestProcessor.AddDefaultPassHeader	This field specifies the header and value that Network Prevent for Email Server adds to each email message that it processes. The default header and value is $X-CFilter-Loop: Reflected. Change$ the value of this field if you want to add a different header to each processed message.
	If you do not want to add a header to each email message, set the AddDefaultPassHeader field to False.

Note: Always configure both RequestProcessor.ServerSocketPort and RequestProcessor.MTAResubmitPort, whether you implement reflecting or forwarding mode. With forwarding mode,

RequestProcessor.ServerSocketPort specifies the SMTP Listener port on the detection server to which the upstream MTA sends email messages. RequestProcessor.MTAResubmitPort is the SMTP Listener port on the downstream MTA to which the detection server sends email messages.

- 9 Click Save.
- 10 Click Done.
- 11 If your email delivery system uses TLS communication in forwarding mode, each next-hop mail server in the proxy chain must support TLS and must authenticate itself to the previous hop. This means that Network Prevent for Email Server must authenticate itself to the upstream MTA, and the next-hop MTA must authenticate itself to Network Prevent for Email Server. Proper authentication requires that each mail server stores the public key certificate for the next hop mail server in its local keystore file.

See "Specifying one or more upstream mail transfer agents (MTAs)" on page 1160.

See "Creating a policy for Network Prevent for Email" on page 1161.

See "Testing Network Prevent for Email" on page 1164.

## Configuring Linux IP tables to reroute traffic from a restricted port

Many Linux systems restrict ports below 1024 to root access. Network Prevent for Email cannot bind to these restricted ports.

If the computer receives mail for inspection on a restricted port (for example, port 25), use the iptables command to route that traffic to a non-restricted port, such as the Network Prevent for Email default port 10025. Then ensure that Network Prevent for Email listens on the non-restricted port to inspect email.

Use the following instructions to configure a Linux system to route from port 25 to port 10025. If you use a different restricted port or Network Prevent for Email port, enter the correct values in the iptables commands.

#### To configure route traffic from port 25 to port 10025

- Configure Network Prevent for Email to use the default port 10025 if necessary. See "Configuring Network Prevent for Email Server for reflecting or forwarding mode" on page 1155.
- In a terminal window on the Network Prevent for Email computer, enter the following commands to reroute traffic from port 25 to port 10025:

```
iptables -N Vontu-INPUT
iptables -A Vontu-INPUT -s 0/0 -p tcp --dport 25 -j ACCEPT
iptables -I INPUT 1 -s 0/0 -p tcp -j Vontu-INPUT
iptables -t nat -I PREROUTING -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
iptables-save > /etc/sysconfig/iptables
```

```
Note: If you only want to test local IP routing between the ports with Telnet,
use the command: iptables -t nat -I OUTPUT -o lo -p tcp
--destination-port 25 -j REDIRECT --to-ports=10025
```

If later you decide to delete the IP tables entry, use the command:

```
iptables -t nat -D OUTPUT -o lo -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
```

## Specifying one or more upstream mail transfer agents (MTAs)

By default, Network Prevent for Email Server can accept connections to the ESMTP service port from any system on the network. You can restrict Network Prevent for Email Server ESMTP communication to a designated set of mail transfer agents (MTAs) for security reasons. Create a "whitelist" of authorized systems. If you whitelist one or more systems, other systems that are not on the whitelist cannot connect to the Network Prevent for Email Server ESMTP service port.

Note that an MTA whitelist might be affected by the

RequestProcessor.BindAddress setting. By default, the

RequestProcessor.BindAddress setting is 0.0.0.0, and the listener binds to all available addresses. If RequestProcessor.BindAddress instructs the listener to bind to a specific IP, a white listed MTA must also be able to reach the listener address.

To create a whitelist of systems allowed to communicate with the Network Prevent for Email Server:

- Go to **System > Servers > Overview** and click on the wanted Network Prevent for Email Server.
- 2 On the Server Detail screen that appears, click Server Settings.
- 3 Scroll down to the **RequestProcessor.AllowHosts** field.
  - By default, RequestProcessor.AllowHosts is set to any, meaning that all other systems on the network can communicate with this Network Prevent for Email Server.
- You can limit the systems that are allowed to connect with this Network Prevent for Email Server. Delete any and enter the IP addresses or FQDN of the systems you want to authorize. Separate multiple addresses with commas. For example:
  - "123.14.251.31, smtp 1.corp.mycompany.com, 123.14.223.111." Separate addresses only with commas; do not include spaces.
- Click Save.

Changes to this setting do not take effect until you restart the server.

## Creating a policy for Network Prevent for Email

You can create the policies that include any of the standard response rules. For example, Add Comment, Limit Incident Data Retention, Log to a Syslog Server, Send Email Notification, and Set Status.

See "Workflow for implementing policies" on page 293.

You can also incorporate the following rules, which are specific to Network Prevent for Email:

#### Network: Block SMTP Message

Blocks the email messages that contain confidential data or significant metadata (as defined in your policies). You can configure Symantec Data Loss Prevention to bounce the message or redirect the message to a specified address. The redirect feature is typically used to reroute messages to the address of a mailbox or mail list. Administrators and managers use the mailbox or list to

review and release messages. Such mailboxes are outside the Symantec Data Loss Prevention system.

#### Network: Modify SMTP Message

Modifies the email messages that contain confidential data or significant metadata (as defined in your policies). You can use this action to modify the message subject or add specific RFC 5322 message headers to trigger further downstream processing. For example, message encryption, message quarantine, or message archiving.

For details on setting up any response rule action, open the online Help. Go to Manage > Policies > Response Rules and click Add Response Rule.

For details on using the **Network: Modify SMTP Message** action to trigger downstream processes (such as message encryption), see the Symantec Data Loss Prevention MTA Integration Guide for Network Prevent.

Even if you do not incorporate response rules into your policy, Network Prevent for Email captures incidents as long as your policies contain detection rules. This feature can be useful if you want to review the types of incidents Symantec Data Loss Prevention captures and to then refine your policies.

#### To create a test policy for Network Prevent for Email

1 In the Enforce Server administration console, create a response rule that includes one of the actions specific to Network Prevent for Email. For example, create a response rule that includes the Network: Block SMTP Message action.

See "Configuring response rules" on page 891.

2 Create a policy that incorporates the response rule you configured in the previous step.

For example, create a policy called Test Policy as follows:

- Include a Content Matches Keyword detection rule that matches on the keyword secret.
- Include a Network: Block SMTP Message response rule.
- Associate it with the Default policy group.

See "Configuring policies" on page 326.

See "About policy violation data headers" on page 1163.

## About policy violation data headers

A message might violate more than one policy. You can add special headers to the outgoing messages that report the number and severity of policies the message violates. Three different kinds of violation-data headers are available:

- Number of violated policies—a header can be added reporting the total number of different policies that the message violates.
- Highest severity—a header can be added reporting the single highest severity level among all policies that the message violates (High, Medium, Low, or Info).
- Cumulative severity score—a header can be added reporting a total severity score which is the numeric sum of all policy violations. For this purpose, severity levels are assigned numeric values: High=4, Medium=3, Low=2, and Info=1. Thus, a message that violates both a Low (2) and Medium (3) severity policy has a total severity score of 5.

You can use headers to trigger downstream responses that are based on the number of violations or the severity of violations. For example:

- Messages that violate a single policy can be routed to one guarantine mailbox. Messages that violate multiple policies can be routed to a second mailbox. Messages that violate over a specified number of policies can be routed to a third mailbox.
- Messages that violate multiple policies can be handled differently according to the severity level of the most serious violation.
- Messages that violate multiple policies can be handled differently according to the total severity score of the message.

See "Enabling policy violation data headers" on page 1163.

## **Enabling policy violation data headers**

Three multiple-policy headers can be used in combination.

To enable policy violation message headers:

- Go to System > Servers > Overview and click on the wanted Network Prevent for Email Server.
- 2 On the **Server Detail** screen that appears, click **Server Settings**.
- 3 Scroll down to one of the three following **RequestProcessor** settings. By default, the value for these settings is false.
- Change the value to true. 4
- 5 Click Save.

Changes to these settings do not take effect until you restart the server.

Three **RequestProcessor** advanced settings enable different kinds of multiple-policy-violation message headers:

- RequestProcessor.TagPolicyCount. When the setting is set to true, Network Prevent adds a header reporting the total number of policies that the message violates. For example, if the message violates 3 policies a header reading: "X-DLP-Policy-Count: 3" is added.
- RequestProcessor.TagHighestSeverity. When the setting is set to true, Network Prevent adds a header reporting the highest severity among the violated policies. For example, if a message violates three policies, one with a severity of "Medium" and two with a severity of "Low" a header reading: "X-DLP-Max-Severity: MEDIUM" is added.
- RequestProcessor.TagScore. When the setting is set to true, Network Prevent adds a header reporting the total cumulative score of all the violated policies. Scores are calculated using the formula: High=4, Medium=3, Low=2, and Info=1. For example, if a message violates three policies, one with a severity of "medium" and two with a severity of "low" a header reading: "X-DLP-Score: 7" is added.

Setting a value to "true" causes the corresponding header to be automatically added to every outgoing message that is processed. This occurs even if the message violates only a single policy.

See "About policy violation data headers" on page 1163.

## **Testing Network Prevent for Email**

You can test Network Prevent for Email by sending an email that violates your test policy.

#### To test your system

- Access an email account that routes messages through an MTA that is integrated with your Network Prevent for Email Server.
- 2 Send an email that contains confidential data. For example, send an email that contains the word Secret.
- In the Enforce Server administration console, go to Incident > Network and click **Incidents - All**. Look for the resulting incident. For example, search for an incident entry that includes the appropriate timestamp and policy name.
- 4 Click on the relevant incident entry to see the complete incident snapshot. See "About Symantec Data Loss Prevention reports" on page 1006.

## Implementing Network Prevent for Web

This chapter includes the following topics:

- Implementing Network Prevent for Web
- Configuring Network Prevent for Web Server
- About proxy server configuration
- Specifying one or more proxy servers
- Enabling GET processing for Network Prevent for Web
- Creating policies for Network Prevent for Web
- Testing Network Prevent for Web
- Troubleshooting information for Network Prevent for Web Server

## Implementing Network Prevent for Web

The Network Prevent for Web Server integrates with an HTTP, HTTPS, or FTP proxy server using ICAP for in-line active Web request management. If it detects confidential data in Web content, it causes the proxy to reject requests or remove HTML content as specified in your policies.

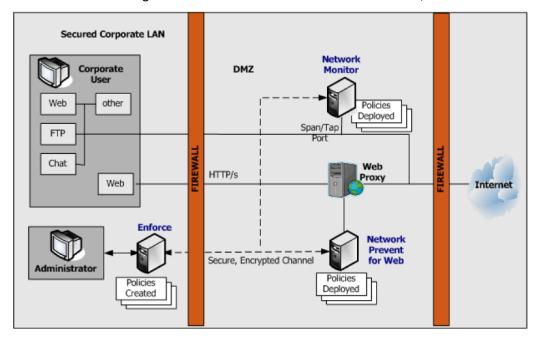


Figure 53-1 A basic Network Prevent for Web setup

First, you need to know the high-level steps that are required for implementing Network Prevent for Web. You can check the cross-referenced sections for more details.

#### To implement Network Prevent for Web

- 1 Make sure the Network Prevent for Web Server is configured to communicate with your HTTP proxy server. Optionally, configure the detection server to filter traffic as wanted.
  - See "Configuring Network Prevent for Web Server" on page 1167.
- Configure your HTTP proxy server to work with the Network Prevent for Web Server.
  - See "About proxy server configuration" on page 1170.
- Create and deploy a policy for Network Prevent for Web.
  - See "Creating policies for Network Prevent for Web" on page 1175.

- Test the system by generating an incident against your test policy. See "Testing Network Prevent for Web" on page 1176.
- 5 If required, troubleshoot the implementation. See "Troubleshooting information for Network Prevent for Web Server" on page 1177.

## Licensing Network Prevent

There are different deployment scenarios for Network Prevent. You can deploy Network Preventas a standalone product, or you can deploy it in conjunction with Mobile Prevent for Web.

Depending on the license that you purchase, the user interface of Symantec Data Loss Prevention changes. What you see on your screen may differ slightly from what is described in the Symantec Data Loss Prevention documentation. The documentation assumes that you are deploying Mobile Prevent and Network Prevent together.

For example, you create a response rule to block sensitive information from transferring over an HTTP protocol. If you have deployed Network Prevent as a standalone product, the Block HTTP/HTTPS response rule action appears under the heading **Network Prevent**. If you have Mobile Prevent and Network Prevent deployed together, the response rule action appears under the heading **Network** and Mobile Prevent for Web.

See "Implementing Mobile Prevent for Web" on page 1542.

## Configuring Network Prevent for Web Server

You can use a number of configuration options for Network Prevent for Web Server. For example, you can configure the server to:

- Ignore small HTTP requests or responses.
- Ignore requests to, or responses, from a particular host or domain (such as the domain of a business subsidiary).
- Ignore user search engine queries.

#### To modify your Network Prevent for Web server configuration

- Go to System > Servers > Overview and click the Network Prevent for Web Server.
- 2 On the **Server Detail** screen that appears, click **Configure**.

You can verify or modify settings on the ICAP tab as described in subsequent steps. The tab is divided into several sections: Request Filtering, Response Filtering, and Connection.

- Verify or change the **Trial Mode** setting. **Trial Mode** lets you test prevention without blocking requests in real time. If you select **Trial Mode**, Symantec Data Loss Prevention detects incidents and indicates that it has blocked an HTTP communication, but it does not block the communication.
- Verify or modify the filter options for requests from HTTP clients (user agents). The options in the **Request Filtering** section are as follows:

Ignore Requests Smaller Than Spec	cifies the minimum body size of HTTP
-----------------------------------	--------------------------------------

requests to inspect. (The default is 4096 bytes.) For example, search-strings typed in to search engines such as Yahoo or Google are usually short. By adjusting this value, you can exclude those searches

from inspection.

Ignore Requests without Attachments Causes the server to inspect only the

> requests that contain attachments. This option can be useful if you are mainly concerned with requests intended to post

sensitive files

Ignore Requests to Hosts or Domains Causes the server to ignore requests to

> the hosts or domains you specify. This option can be useful if you expect a lot of HTTP traffic between the domains of your corporate headquarters and branch offices. You can type one or more host or domain names (for example, www.company.com),

each on its own line.

Ignore Requests from User Agents Causes the server to ignore requests from

user agents (HTTP clients) you specify. This option can be useful if your organization uses a program or language (such as Java) that makes frequent HTTP requests. You can type one or more user agent values, each on its own line.

5 Verify or modify the filter options for responses from Web servers. The options in the **Response Filtering** section are as follows:

Ignore Responses Smaller Than Specifies the minimum size of the body of

HTTP responses that are inspected by this

server. (Default is 4096 bytes.)

**Inspect Content Type** Specifies the MIME content types that

> Symantec Data Loss Prevention should monitor in responses. By default, this field contains content-type values for Microsoft Office, PDF, and plain text formats. To add others, type one MIME content type per

line. For example, type

application/word2013 to have Symantec Data Loss Prevention analyze

Microsoft Word 2013 files.

Note that it is generally more efficient to specify MIME content types at the Web

proxy level.

Ignore Responses from Hosts or

**Domains** 

Causes the server to ignore responses from the hosts or domains you specify. You can type one or more host or domain names (for example, www.company.com),

each on its own line.

Ignore Responses to User Agents Causes the server to ignore responses to

> user agents (HTTP clients) you specify. You can type one or more user agent

values, each on its own line.

Verify or modify settings for the ICAP connection between the HTTP proxy server and the Web Prevent Server. The **Connection** options are as follows:

TCP Port Specifies the TCP port number over which

> this server listens for ICAP requests. This number must match the value that is configured on the HTTP proxy that sends ICAP requests to this server. The

recommended value is 1344

**Maximum Number of Requests** Specifies the maximum number of

> simultaneous ICAP request connections from the HTTP proxy or proxies. The

default is 25.

Specifies the maximum number of **Maximum Number of Responses** 

> simultaneous ICAP response connections from the HTTP proxy or proxies. The

default is 25.

Connection Backlog Specifies the number of waiting

> connections allowed. A waiting connection is a user waiting for an HTTP response from the browser. The minimum value is 1. If the HTTP proxy gets too many requests (or responses), the proxy handles them according to your proxy configuration. You can configure the HTTP proxy to block any requests (or responses) greater than

this number.

Click Save to exit the Configure Server screen and then click Done to exit the Server Detail screen.

## About proxy server configuration

You must configure at least one HTTP proxy server to forward Web requests or responses to the Mobile Prevent for Web Server. The HTTP proxy acts as an ICAP client to the Network Prevent for Web Server. Symantec Data Loss Prevention supports both the request modification (REQMOD) and response modification (RESPMOD) modes of ICAP. If you want to analyze requests as well as responses, use one Network Prevent for Web Server to analyze requests. Use a second Network Prevent for Web Server to analyze responses.

Note that most proxy servers provide methods of filtering what is forwarded to the Network Prevent for Web Server in both REQMOD mode and RESPMOD modes. Consult the proxy server's documentation for details.

See "Specifying one or more proxy servers" on page 1173.

See "Proxy server compatibility with Network Prevent for Web" on page 1171.

See "Configuring request and response mode services" on page 1172.

## Proxy server compatibility with Network Prevent for Web

Network Prevent for Web Servers use the ICAP protocol and can operate with the following proxies:

Table 53-1 Network Prevent for Web supported proxy servers

Proxy	Supported protocols	Configuration information
Blue Coat ProxySG version 4.2.1, 5.2.4.8, 5.5.2.1, 5.5.3.1, 6.2.12.1, and 6.5.x for Network Prevent for Web	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Blue Coat product documentation
Blue Coat ProxySG version 5.5.3.1 for Mobile Prevent		
Cisco IronPort S-Series version 6.0, 7.1.2	HTTP, HTTPS, FTP over HTTP	Cisco IronPort product documentation
Microsoft TMG 2010 (without service pack, or with SP1 or SP2) on Microsoft Windows 2008 R2 SP1 Enterprise or Standard Edition	HTTP, HTTPS, limited FTP over HTTP/S	See the Symantec Data Loss Prevention Integration Guide for Microsoft Threat Management Gateway
Secure Computing Secure Web (Webwasher) versions 6.9.x, 7.2, and 7.4	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Secure Web documentation (particularly the chapter that describes setting up Secure Web with a DLP Solution)
Squid Web Proxy version 3.0 Stable 18 through 3.1.11, 3.3.5 (Linux only)	нттр	See the Symantec Data Loss Prevention Integration Guide for Squid Web Proxy
Symantec Web Gateway versions 5.0 and 5.0.2.8	нттр, нттрs	See the Symantec Web Gateway 5.0 Implementation Guide

Proxy	Supported protocols	Configuration information
Websense Appliance V5000 and V10000, with Websense Web Security version 7.6.0	HTTP, HTTPS	Does not support redaction.  Only supports "Block HTTP/HTTPS".  RESPMOD is not supported.  Websense blocks the traffic only when the size of the Symantec Data Loss Prevention rejection message (in the response rule) is larger than 512 bytes. If the rejection message is less than 512 bytes, an incident is generated but the network traffic is not blocked.

Table 53-1 Network Prevent for Web supported proxy servers (continued)

See "Specifying one or more proxy servers" on page 1173.

See "About proxy server configuration" on page 1170.

## Configuring request and response mode services

For details on configuring the proxy server, refer to your proxy server product documentation, or contact your proxy server administrator.

#### To configure a proxy server:

REQMOD. On your proxy server, create an ICAP REQMOD service that forwards requests to the Mobile Prevent for Web Server. If your proxy server supports different protocols, configure it to handle the wanted protocols.

For REQMOD mode, an ICAP service on the proxy server should look like:

icap://ip address|FQDN[:port]/reqmod

RESPMOD. On your proxy server, create an ICAP RESPMOD service that forwards responses to the Mobile Prevent for Web Server. If your proxy server supports different protocols, configure it to handle the wanted protocols.

For RESPMOD mode, an ICAP service on the proxy server should look like:

icap://ip address|FQND[:port]/respmod

#### Where:

■ ip\_address|FQDN identifies the Mobile Prevent for Web Server using either an IP address or fully qualified domain name.

- Port is the port number to which Mobile Prevent for Web Server listens. Specifying the port number is optional when the default ICAP port (1344) is used.
- /regmod is required for correct functionality in REQMOD mode.
- /respmod is required for correct functionality in RESPMOD mode.

#### Examples:

```
icap://10.66.194.45/reqmod
icap://10.66.194.45:1344/reqmod
icap://netmonitor1.company.com/reqmod
icap://10.66.194.45/respmod
icap://10.66.194.45:1344/respmod
icap://netmonitor1.company.com/respmod
```

Note that the port that is specified in the ICAP service definition on the proxy must match the port on which Mobile Prevent for Web Server listens.

See "Proxy server compatibility with Network Prevent for Web" on page 1171.

See "About proxy server configuration" on page 1170.

## Specifying one or more proxy servers

By default, Network Prevent for Web Server can accept connections to the ICAP service port from any system on the network. For security reasons, you can limit ICAP connections to only those systems that you designate (or "whitelist"). Once you whitelist one or more systems, systems not on the whitelist cannot connect to the Network Prevent for Web Server ICAP service port.

Note that a proxy server whitelist can be affected by the Icap.BindAddress setting. By default, the Icap.BindAddress settings is 0.0.0.0, and the listener binds to all available addresses. If Icap.BindAddress instructs the listener to bind to a specific IP, a white listed proxy must also be able to reach the listener address.

To create a whitelist of systems allowed to make a connection to the Network **Prevent for Web server ICAP service port:** 

- Go to System > Servers > Overview and click on the wanted Network Prevent for Web Server.
- 2 On the Server Detail screen that appears, click Server Settings.
- 3 Scroll down to the **lcap.AllowHosts** setting.

By default, Icap.AllowHosts is set to any, meaning that all other systems on the network can communicate with this Network Prevent for Web Server.

You can limit the systems that are allowed to connect with this Network Prevent for Web Server. Delete any and enter the IP addresses or Fully-Qualified Domain Name (FQDN) of the systems you want to authorize.

Separate multiple addresses with commas. For example: 123.14.251.31, webcache.corp.mycompany.com, 123.14.223.111. Use only commas to separate multiple entries; do not include spaces.

5 Click Save.

Changes to this setting do not take effect until you restart the server.

See "Proxy server compatibility with Network Prevent for Web" on page 1171.

See "About proxy server configuration" on page 1170.

## **Enabling GET processing for Network Prevent for Web**

By default, Network Prevent for Web does not process HTTP GET commands because of the high traffic volume. Follow this procedure to enable the server to process GET commands.

#### To enable GET processing with Network Prevent for Web

- Configure the Web proxy server to forward GET requests to the Network Prevent for Web Server as described in your proxy server documentation.
- 2 Ensure that the L7.processGets advanced server setting on the Network Prevent for Web Server must be "true" (which is the default).
- Reduce the size of the L7.minSizeofGetURL Advanced setting on the Network 3 Prevent for Web Server. Reduce from the default of 100 to a number of bytes smaller than the length of the shortest Web site URL from which you want to process GET commands. A minimum URL size to 10 should cover all cases. Note, however, that reducing the minimum size of GETs increases the number of requests that have to be processed, which increases the server traffic load.
- Adjust the **Ignore Requests Smaller Than** setting in the ICAP section of the Network Prevent for Web Server Detail page. Reduce it from the default of 4096 bytes to a lower value that would enable the request to undergo DLP inspection. Note, however, that lowering the value increases the server traffic load.

See "Enabling GET processing with Network Monitor" on page 1149.

## **Creating policies for Network Prevent for Web**

You can create the policies that include any of the standard response rules. For example, Add Comment, Limit Incident Data Retention, Log to a Syslog Server, Send Email Notification, and Set Status.

See "About Symantec Data Loss Prevention reports" on page 1006.

You can also incorporate the rules that are specific to Network Prevent for Web Server as follows:

#### **Network Prevent: Block HTTP/HTTPS**

Blocks posts that contain confidential data (as defined in your policies). This includes Web postings, Web-based email messages, and files that are uploaded to Web sites or attached to Web-based email messages.

Note: Certain applications may not provide an adequate response to the **Network** Prevent: Block HTTP/HTTPS response action. This behavior has been observed with the Yahoo! Mail application when a detection server blocks a file upload. If a user tries to upload an email attachment and the attachment triggers a Network Prevent: Block HTTP/HTTPS response action, Yahoo! Mail does not respond or display an error message to indicate that the file is blocked. Instead, Yahoo! Mail appears to continue uploading the selected file, but the upload never completes. The user must manually cancel the upload at some point by pressing Cancel.

Other applications may also exhibit this behavior, depending on how they handle the block request. In these cases a detection server incident is created and the file upload is blocked even though the application provides no such indication.

#### **Network Prevent: Remove HTTP/HTTPS Content**

Removes confidential data from posts that contain confidential data (as defined in your policies). This includes Web-based email messages and files that are uploaded to Web sites or attached to Web-based email messages. Note that the Remove HTTP/HTTPS Content action works only on requests.

### **Network Prevent: Block FTP Request** Blocks FTP transfers that contain confidential data (as defined in your policies).

For details on setting up any response rule action, open the online Help. Go to Manage > Policies > Response Rules and click Add Response Rule.

Even if you do not incorporate response rules into your policy, Network Prevent for Web captures incidents as long as your policies contain detection rules. You can set up such policies to monitor Web and FTP activity on your network before implementing the policies that block or remove content.

If you have configured your proxy to forward both HTTP/HTTPS requests and responses, your policies work on both. For example, policies are applied to both an upload to a Web site and a download from a Web site.

#### To create a test policy for Network Prevent for Web

1 In the Enforce Server administration console, create a response rule that includes one of the actions specific to Network Prevent for Web. For example, create a response rule that includes the Network Prevent: Block HTTP/HTTPS action.

See "Configuring response rules" on page 891.

Create a policy that incorporates the response rule you configured in the previous step.

For example, create a policy called Test Policy as follows:

- Include a Content Matches Keyword detection rule that matches on the keyword secret.
- Include a **Network Prevent: Block HTTP/HTTPS** response rule.
- Associate it with the Default policy group.

See "Configuring policies" on page 326.

## Testing Network Prevent for Web

You can test Network Prevent for Web by sending a Web email that violates your test policy.

#### To test your system

- Open a browser that accesses the Internet through your HTTP proxy server.
- In the browser, access a test Web email account and send an email with an attachment containing confidential data. For example, access an account in Hotmail and send an email with an attachment containing the word Secret and paragraphs of other text.
- In the Enforce Server administration console, go to Incidents > Network and click Incidents - All. Look for the resulting incident. For example, search for an incident entry that includes the appropriate timestamp and policy name.
- Click on the relevant incident entry to see the complete incident snapshot. See "About strategies for using reports" on page 1007.

## **Troubleshooting information for Network Prevent for Web Server**

The following table describes a common problem when using Network Prevent for Web Server and suggests a possible solution.

**Table 53-2** Troubleshooting

Problem	Possible Solution
Incidents appear in Network reports, but Symantec Data Loss Prevention does not perform the action specified in the relevant response rule.	This is expected behavior when the Network Prevent for Web Server is running in trial mode (the default setting). If you do not want to run in trial mode, change the setting.
	See "Configuring Network Prevent for Web Server" on page 1167.

Section

# Discovering where confidential data is stored

- Chapter 54. About Network Discover
- Chapter 55. Setting up and configuring Network Discover
- Chapter 56. Network Discover scan target configuration options
- Chapter 57. Managing Network Discover target scans
- Chapter 58. Using Server FlexResponse plug-ins to remediate incidents
- Chapter 59. Setting up scans of file shares
- Chapter 60. Setting up scans of Lotus Notes databases
- Chapter 61. Setting up scans of SQL databases
- Chapter 62. Setting up scans of SharePoint servers
- Chapter 63. Setting up scans of Exchange servers
- Chapter 64. About Network Discover scanners
- Chapter 65. Setting up scanning of file systems
- Chapter 66. Setting up scanning of Web servers

- Chapter 67. Setting up scanning of Documentum repositories
- Chapter 68. Setting up scanning of Livelink repositories
- Chapter 69. Setting up Web Services for custom scan targets

## About Network Discover

This chapter includes the following topics:

- About Network Discover
- How Network Discover works

### **About Network Discover**

Network Discover locates the exposed confidential data by scanning a broad range of enterprise data repositories. These data repositories include file servers, databases, Microsoft SharePoint, Lotus Notes, Documentum, Livelink, Microsoft Exchange, Web servers, and other data repositories.

Network Discover can scan the following data sources:

- Network file shares (CIFS, NFS, or DFS)
   See "Setting up server scans of file systems" on page 1241.
- Local file systems on Windows desktops and laptops
   Local file systems on Windows, Linux, AIX, and Solaris servers
   See "Setting up remote scanning of file systems" on page 1315.
- Lotus Notes Databases
   See "Setting up server scans of Lotus Notes databases" on page 1261.
- SQL Databases
   See "Setting up server scans of SQL databases" on page 1267.
- SharePoint 2007 and 2010 servers
   See "Setting up server scans of SharePoint servers" on page 1274.
- Microsoft Exchange Servers
   See "Setting up server scans of 2007 repositories using the Exchange Web Store connector" on page 1287.

See "Setting up server scans of Exchange 2007 SP2 and 2010 repositories using Exchange Web Services" on page 1295.

Documentum

See "Setting up remote scanning of Documentum repositories" on page 1339.

Livelink

See "Setting up remote scanning of Livelink repositories" on page 1348.

- Web servers (Web sites and Web-based applications) See "Setting up remote scanning of Web servers" on page 1327.
- Web services

Web services expose a custom integration point. You can write custom code to scan any repository. The custom code crawls the repository and feeds the content to a Network Discover Server for scanning. Custom applications and repositories can be scanned with Web services.

See "Setting up Web Services for custom scan targets" on page 1356.

Custom

Custom applications can be written that extract content and metadata from a repository and feed them to Network Discover. The recommended Network Discover interface for custom integration is Web services.

Endpoint Discover can scan file systems on Windows desktop or laptop computers. Endpoint Discover includes an agent on the Windows desktop or laptop computer that scans the local file system.

During incident remediation, Symantec Data Insight helps organizations solve the problem of identifying data owners and responsible parties for information due to incomplete or inaccurate metadata or tracking information.

With Symantec Data Insight, users can monitor file access to automatically identify the data user of a file based on the access history. The usage information then automatically feeds into the incident detail of files that violate Symantec Data Loss Prevention policies. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

See the Symantec Data Loss Prevention Data Insight Implementation Guide.

The FlexResponse Platform enables the creation of comprehensive custom remediation actions for the files that are discovered using Symantec Data Loss Prevention Network Discover. FlexResponse supports Symantec and third-party file security solutions including Enterprise Digital Rights Management and encryption. FlexResponse is an extension of the Network Protect product, and the Network Protect product is required for FlexResponse functionality.

See the Symantec Data Loss Prevention FlexResponse Developers Guide, or contact Symantec Data Loss Prevention Professional Services for a list of available plug-ins.

During incident remediation, you can use the installed FlexResponse plug-ins to remediate incidents.

See "Using Server FlexResponse custom plug-ins to remediate incidents" on page 1230.

## How Network Discover works

The Network Discover Server locates a wide range of exposed confidential data. It communicates with the Enforce Server to obtain information about policies and scan targets. It sends information about the exposed confidential data that it finds to the Enforce Server for reporting and remediation.

Figure 54-1 shows the Network Discover Server securely inside the corporate LAN.

The Network Discover Server is connected to the Enforce Server and each server performs the tasks that are related to locating exposed confidential data.

Multiple Network Discover Servers can be set up to spread out the work.

See "Adding a detection server" on page 194.

The Network Discover Server scans the selected targets, reads the files or repositories, and detects whether confidential information is present.

The Enforce Server contains the user interface where the following tasks are done:

- Setting up target scans.
- Selecting target repositories.
- Defining filters for the scans.
- Scheduling scans.

See "Adding a new Network Discover target" on page 1187.

The Enforce Server also manages the scans running on the Network Discover Servers and displays the status of the scans in the user interface.

See "Managing Network Discover target scans" on page 1209.

After a scan is complete, you can display the reports of the exposed confidential data on the Enforce Server.

See "About reports for Network Discover" on page 988.

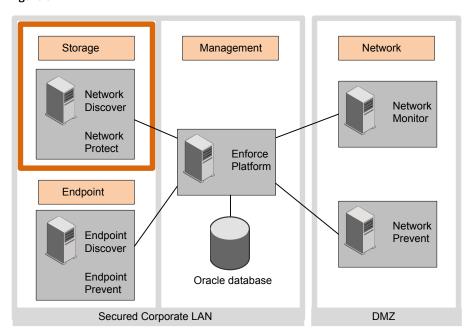


Figure 54-1 **Network Discover** 

## Setting up and configuring Network Discover

This chapter includes the following topics:

- Setting up and configuring Network Discover
- Modifying the Network Discover Server configuration
- About Linux Network Discover Servers
- Adding a new Network Discover target
- Editing an existing Network Discover target

## Setting up and configuring Network Discover

Setting up a Network Discover scan target involves several steps. Each of these steps is necessary to correctly implement Network Discover target scanning.

**Table 55-1** Setting up and Configuring Network Discover

Step	Action	Details
1	Modify the Network Discover Server configuration, if needed.	See "Modifying the Network Discover Server configuration" on page 1185.
2	Create a policy group.	Go to System > Servers > Policy Groups.
		On the <b>Policy Group List</b> screen that appears, click <b>Add Policy Group</b> .
		See "Creating and modifying policy groups" on page 348.

Step	Action	Details
3	Create a policy.	Go to <b>Manage &gt; Policies &gt; Policy List</b> on the Enforce Server.
		Select Add a blank policy.
		Add a rule to the policy.
		See "Configuring policies" on page 326.
4	Before using Network Protect for a file share Discover target, create a response rule. Using Network Protect is optional.	See "About response rules" on page 875.
5	Create a Network Discover Target.	Go to Manage > Discover Scanning > Discover Targets on the Enforce Server.
		Click <b>New Target</b> , and use the pull-down menu to select the specific target type.
		See "Adding a new Network Discover target" on page 1187.
6	Set options for the target.	See "Network Discover scan target configuration options" on page 1191.
7	Set up reports.	See "About Symantec Data Loss Prevention reports" on page 1006.

Table 55-1 Setting up and Configuring Network Discover (continued)

## Modifying the Network Discover Server configuration

After you have installed your Network Discover Servers and registered them with the Enforce Server, you can modify the Network Discover Server configuration.

If your Network Discover Server is installed on a Linux system, note the differences from a Network Discover Server on a Windows system.

See "About Linux Network Discover Servers" on page 1187.

The Network Discover Server can be installed on a virtual machine. For the supported virtual machines types, see the Symantec Data Loss Prevention System Requirements and Compatibility Guide.

If you have configured incremental scanning, the incremental scan index is automatically distributed to all Discover Servers, including any new Discover Servers. See "About incremental scans" on page 1223.

#### To modify a Network Discover Server configuration

In the Enforce Server administration console, go to System > Servers > Overview. Then click the server to modify.

The appropriate Server Detail screen appears and displays general server information, configuration information, deployed indexes, and recent server events.

#### 2 Click Configure.

The Configure Server screen appears and displays configuration options for the server type.

Modify the server configuration. 3

The following configuration options are on the **General** tab:

#### Name

The name of the detection server (used for displays in the Enforce Server administration console). Changing this setting for an existing detection server affects your filter options in Symantec Data Loss Prevention reports. Network Discover Servers are detection servers.

#### Host

The detection server host name or IP address on which the detection server listens for connections to the Enforce Server. You might need to modify this setting when you replace a Network Discover Server host computer.

#### Port

The detection server uses the port number to accept connections from the Enforce Server. This value must be greater than 1024. It must also match the value of the listenPort property in the detection server's Communication.properties file. This file is located in SymantecDLP\Protect\config. If you change this setting, restart the detection server after modifying the listenPort value in the Communication.properties file. You should not need to change this setting after a successful installation.

See "Server controls" on page 178.

The configuration for parallel scanning is on the **Discover** tab. Enter the number of parallel scans to run on this Network Discover Server. The default is 1.

The maximum count can be increased at any time. After it is increased, then any queued scans that are eligible to run on this Network Discover Server are started.

The count can be decreased only if the Network Discover Server has no running scans. Before you reduce the count, pause or stop all scans on the Network Discover Server.

Parallel scans of server and scanner target types are supported. Parallel scanning of Endpoint file systems is not supported.

See "Configuring parallel scanning of Network Discover targets" on page 1226.

- 5 When you finish modifying a server configuration, click **Save** to exit the **Configure Server** screen and then click **Done** to exit the Server Detail screen.
- To view the active scans on this Network Discover Server, go to **Policies >** Discover Scanning > Discover Servers.

See "Managing Network Discover target scans" on page 1209.

## About Linux Network Discover Servers

If your Network Discover Server is installed on a Linux system, note the following differences from a Network Discover Server on a Windows system:

- The date Last Accessed of a file cannot be reset after it is scanned.
- The **Owner** and date **Last Accessed** of the violating file cannot be retrieved. The Access Control Lists (ACLs) are retrieved correctly.
- You cannot scan Microsoft Outlook Personal Folders (.pst) files.
- SFTP scanning is not supported.
- A Network Discover Server on Linux uses iCIFS which is limited to a single-thread. Scans may be slower than on a Windows Network Discover Server.

See "Setting up and configuring Network Discover" on page 1184.

## Adding a new Network Discover target

Before adding a Network Discover target, you must complete the Network Discover Server setup.

See "Setting up and configuring Network Discover" on page 1184.

#### To add a Network Discover target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click New Target, and use the pull-down menu to select the specific target 2 type.
- 3 On the **General** tab, enter the name of this Network Discover target. This name displays for management of scans.
  - See "Managing Network Discover target scans" on page 1209.
- 4 Enter the remaining required parameters. Enter the policy group. Enter the Network Discover Server.
  - See "Configuring the required fields for Network Discover targets" on page 1193.

5 Continue the addition of a new target, with the entries specific to that target type.

Network file servers and shares (CIFS,

NFS. DFS)

See "Setting up server scans of file

systems" on page 1241.

Lotus Notes databases

See "Setting up server scans of Lotus Notes databases" on page 1261.

SQL databases

See "Setting up server scans of SQL

databases" on page 1267.

Local file systems on Windows desktops

and laptops

See "Setting up remote scanning of file

systems" on page 1315.

Local file systems on Windows, Linux, AIX,

and Solaris servers

Microsoft Exchange See "Setting up server scans of 2007

repositories using the Exchange Web Store

connector" on page 1287.

See "Setting up server scans of Exchange 2007 SP2 and 2010 repositories using Exchange Web Services" on page 1295.

SharePoint See "Setting up server scans of SharePoint

servers" on page 1274.

Documentum See "Setting up remote scanning of

Documentum repositories" on page 1339.

Livelink See "Setting up remote scanning of Livelink

repositories" on page 1348.

Web servers (Web sites and Web-based

applications)

See "Setting up remote scanning of Web

servers" on page 1327.

Configure optional Network Discover target parameters.

See "Network Discover scan target configuration options" on page 1191.

# **Editing an existing Network Discover target**

To set various configuration options, edit the configuration of a Network Discover target.

You can also add a new Network Discover target, and set options at that time.

See "Adding a new Network Discover target" on page 1187.

## To edit a Network Discover target

- 1 In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click one of the scan targets from the list to open the target for editing.
- 3 Edit the desired option.

See "Network Discover scan target configuration options" on page 1191.

# Network Discover scan target configuration options

This chapter includes the following topics:

- Network Discover scan target configuration options
- Configuring the required fields for Network Discover targets
- Scheduling Network Discover scans
- Providing the password authentication for Network Discover scanned content
- Encrypting passwords in configuration files
- Setting up Network Discover filters to include or exclude items from the scan
- Filtering Discover targets by item size
- Filtering Discover targets by date last accessed or modified
- Optimizing resources with Network Discover scan throttling
- Creating an inventory of the locations of unprotected sensitive data

## **Network Discover scan target configuration options**

Use the **General**, **Scanned Content**, **Filters**, and **Advanced** tabs to configure a Network Discover scan target.

The **General** tab is available for all types of targets.

The **Scanned Content**, **Filters**, and **Advanced** tabs are only available for some types of targets.

See "Editing an existing Network Discover target" on page 1189.

For the additional configuration information that is specific to one type of target, refer to the section for that target type.

Note that all filters are combined with "and" if a value is provided. Consider all filter values when adding or modifying scan filters, to avoid unintentionally including or excluding everything from the scan.

For configuration when adding or editing a target, select from the following options:

Optional tasks	Tab in scan target	Description of task
Configure required fields.	General	See "Configuring the required
These required fields should be set when a new target is added.		fields for Network Discover targets" on page 1193.
Schedule Network Discover scans.	General	See "Scheduling Network Discover scans" on page 1194.
Configure incremental scans.	General	See "Scanning new or modified items with incremental scans" on page 1224.
Provide authentication, and set up credentials.	Scanned Content	See "Providing the password authentication for Network Discover scanned content" on page 1196.
Include, or exclude, repositories from a scan.	Filters	See "Setting up Network Discover filters to include or exclude items from the scan" on page 1198.
Filter targets by file size.	Filters	See "Filtering Discover targets by item size" on page 1201.
Filter targets by date last accessed or modified.	Filters	See "Filtering Discover targets by date last accessed or modified" on page 1202.
Optimize your resources with scan throttling.	Advanced	See "Optimizing resources with Network Discover scan throttling" on page 1204.
Create an inventory of the locations of unprotected sensitive data.	Advanced	See "Creating an inventory of the locations of unprotected sensitive data" on page 1206.

Optional tasks	Tab in scan target	Description of task
Specify options for automatically tracking remediation status for network file system incidents.	Advanced	See "Configuring and running scans of file systems" on page 1254.
Move or quarantine files in network file shares with Network Protect.	Protect	See "Configuring Network Protect for file shares" on page 1258.

# Configuring the required fields for Network Discover targets

For a new target, enter the name of the target, the policy group, and the Discover Server where the scans can run.

These required fields should be set when a new target is added.

## To enter the required fields for a target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click **New Target**, and use the pull-down menu to select the specific target type.
- On the **General** tab, enter the **Name** of this Discover target.

Enter a unique name for the target, or edit the existing name, up to 255 characters.

## Select the **Policy Group**.

If no other policy group has been selected, the Default Policy group is used. To apply a policy group, select the policy group to use for this target. You can assign multiple policy groups to a target.

The administrator defines policy groups on the Policy Group List page. If the policy group you want to use does not appear on the list, contact your Symantec Data Loss Prevention administrator.

- 5 Select the Discover Server (or multiple Discover Servers) where you want to allow the scan to run.
  - If you select more than one server, Symantec Data Loss Prevention automatically selects one of the servers when the scan starts.
  - Only the detection servers that were configured as Discover Servers appear on the list. If there is only one Discover Server on your network, the name of that server is automatically specified. You should configure your Discover Servers before you configure targets. You must specify at least one server before you can run a scan for this target.
- On the **Scanned Content** tab, you must enter the item to be scanned. Refer to the documentation about each type of target for additional information about this entry.
  - See "About Network Discover" on page 1180.
- You can configure other options for this target.
  - See "Network Discover scan target configuration options" on page 1191.

## **Scheduling Network Discover scans**

Network Discover scans can be set up to run on a regular schedule, for example during nights or weekends. Scans can also be set to pause during specified times, for example when resources are normally busy with other tasks.

For file shares, Lotus Notes, or SQL databases, the scan schedule can be completely specified with the Scan Schedule parameters.

For the scanner targets (such as SharePoint or Exchange), the scan must also be scheduled from the computer where the scanner is installed. You must manually manage the scan schedule between the Discover target and the scanner application. The scanners are installed, configured, and run outside of the Enforce Server and Network Discover Server. For example, the scanner can be scheduled to run automatically using the host's native scheduling. You can create a UNIX cron job, or add the scanner to the Windows scheduler. The scanner should be scheduled to run before the scheduled Network Discover scan, so that the Network Discover scan has information to consume.

If you select a specific time for starting or pausing a scan, the time zone of the Enforce Server is used.

You can configure other options for this target.

See "Network Discover scan target configuration options" on page 1191.

### To set up a scan schedule

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click the name of the scan that you want to schedule.
- 3 Click the **General** tab.
- Select the item Submit Scan Job on Schedule.

When you select this check box to set up a schedule for scanning the specified target, the Schedule drop-down list becomes available. After you select an option from the Schedule drop-down list, additional fields appear.

5 Select one of the following additional fields:

No Regular Schedule Save the target without a schedule.

Scan Once Run the scan one time, at the specified

time and date.

Scan the target daily, at the specified start Scan Daily

time. Check **Until** to stop the daily scan

after a certain date.

Scan Weekly Scan the target every week. Check Until

to stop the weekly scan after a certain date.

Scan Monthly Scan the target every month. Check Until

to stop the monthly scan after a certain

date.

#### 6 Click Save.

### To pause a scan during specified times

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click the name of the scan that you want to pause during specified times.
- 3 Click the **General** tab.
- 4 Select the item Pause Scan between these times.

#### 5 Select the pause options.

This option automatically pauses scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the scan window pause as specified. You can also restart a paused scan by clicking the continue icon in the target entry.

Note: If the target configuration is modified while it is paused, then the modified configuration does not apply to items that were already scanned. When a scan is paused and restarted, the scan is restarted from a checkpoint that is created when the scan is paused. The modified configuration is used for the items that are scanned from that checkpoint.

6 Click Save.

## Providing the password authentication for Network Discover scanned content

On the **Scanned Content** tab, enter the configuration options for authentication.

Avoid special characters in the authentication credentials. Authentication credentials must not contain any of the following characters, or the scan fails:

- Pipe character
- Ampersand character
- Quotation marks (single or double)

## To provide password authentication for scanned content

- In the Enforce Server administration console, go to **Manage > Discover** Scanning > Discover Targets.
- 2 Click the name of the scan to provide the password authentication.
- Click the Scanned Content tab. 3
- You can enter authentication information in several ways:
  - Use a stored credential. If a stored credential is available, select a named credential from the drop-down in Use Saved Credentials.
  - A global scan credential can be provided for all shares in this target.

Enter the user name and password in **Use These Credentials**.

Separate authentication credentials can be provided for each share in a

A separate credential supersedes the global scan credential, if one was provided.

Click **Add** or **Edit** to provide credentials for each share in a list. In the **Add** box, enter the share and credentials with the following syntax: path[, [username, password][, [depth][, remediation-username, remediation-password[]]

For omitted items, provide a null entry with consecutive commas.

5 The format of the credentials depends on the type of scan. For the specific format and examples of credentials for each target type, see the topic for that target type.

See "About Network Discover" on page 1180.

6 You can set other options on the **Scanned Content** tab.

See "Network Discover scan target configuration options" on page 1191.

Remediation credentials can be set on the **Protect** tab.

See "Configuring Network Protect for file shares" on page 1258.

## **Encrypting passwords in configuration files**

Encrypt passwords in the configuration files with the utility EncryptPassword.exe.

## To encrypt passwords in configuration files

Navigate to the bin directory of the scanner installation on the scanner computer.

See "Scanner installation directory structure" on page 1309.

2 Run the utility EncryptPassword.exe.

> This utility encrypts the password that is provided in the scanner configuration files.

- 3 When the utility requires you to enter a password, enter a password.
- 4 Click the encrypt option.
- Place the encrypted password into the Password= setting in the Vontuscanner typeScanner.cfg file.

See "Configuration options for Web server scanners" on page 1332.

See "Configuration options for Documentum scanners" on page 1344.

See "Configuration options for Livelink scanners" on page 1354.

# Setting up Network Discover filters to include or exclude items from the scan

Exclude and include filters reduce the number of items or repositories to scan.

Use the **Include Filters** field to specify the items that Symantec Data Loss Prevention should process. If you leave the **Include Filters** field empty, Symantec Data Loss Prevention performs matching on all items in the selected target. If you enter any values in the field, Symantec Data Loss Prevention scans only those items that match your filter.

Use the **Exclude Filters** field to specify the items that Symantec Data Loss Prevention should not process. If you leave the **Exclude Filters** field empty, Symantec Data Loss Prevention performs matching on all items in the selected target. If you enter any values in the field, Symantec Data Loss Prevention scans only those items that do not match your filter.

To optimize scanning, you can break up scans using include and exclude filters. For example, you can exclude binary items. Binary items are less likely to contain policy violations.

See "About Network Discover scan optimization" on page 1220.

Note that all filters are combined with "and" if a value is provided. Consider all filter values (for example size and date) when adding or modifying scan filters. Avoid unintentionally including everything, or excluding everything from the scan.

See "Network Discover scan target configuration options" on page 1191.

## To set up include filters or exclude filters:

- In the Enforce Server administration console, go to **Manage > Discover** Scanning > Discover Targets.
- 2 Click the name of the scan where you want to add include filters or exclude filters.
- Click the **Filters** tab.

Enter file names or paths into the include filters and the exclude filters to select a subset of items that Symantec Data Loss Prevention should process. Delimit entries with a comma, but no spaces. The path filter is case-sensitive.

When both include filters and exclude filters are present, exclude filters take precedence.

The include filter and exclude filter file names are relative to the file system root. Specify full paths or subdirectories, as needed. Some wildcards are allowed.

Table 56-1 shows the syntax for the filters.

If the exclude filter entry exceeds the 1024-character limit, you can create an exclude file with the file names to be excluded.

#### 5 Click Save.

#### To create an exclude file:

Create a directory named excludeFiles in the Symantec Data Loss Prevention configuration directory, for

example\SymantecDLP\Protect\config\excludeFiles\.

For a configuration with multiple Discover servers, a copy of this directory and file must be present on each Discover server.

- 2 In this directory create one text file for each set of items to exclude.
  - For example, you can create one file for each UNIX system to be scanned. Name the files hostname.txt, where hostname is the name of the system to be scanned, as provided in the target configuration. The host name in this text file must match exactly the name that is in the Network Discover target.
- In each file, list the paths (each path on a separate line) that you want to exclude from the scan.

The paths can be files, directories, symbolic links, or mounted directories. The paths must each begin with a delimiter of "/" or "\" followed by the share name, directory name, and file name. For example, a valid path is

\excludeshare\excludedir\excludefile.

Table 56-1 shows the syntax for filters.

Table 56-1 Syntax for the include filters and exclude filters

Wildcard	Description
* (asterisk)	Use this wildcard to match any sequence of characters, including null.

**Table 56-1** Syntax for the include filters and exclude filters (continued)

Wildcard	Description
? (question mark)	Use this wildcard to match any one character in the place where it appears.
, (comma)	Represents a logical OR. Delimit entries with a comma, but do not use any spaces.
The forward slash (/) and backslash (\) characters	These characters are equivalent. They usually represent directory separators, although on Linux the backslash is a valid character in a file name.
White space at the beginning and end of the pattern	White space is ignored at the beginning and end of the pattern. Do not use spaces before or after the commas that delimit entries.
Escape characters	The matching process does not support escape characters, so there is no way to match a question mark, a comma, or an asterisk explicitly. In general, special characters in filter items are not supported.

Table 56-2 shows the example filters.

Example filters using wildcards Table 56-2

Example filter	Description
*.txt,*.doc	This example of an include filter matches only files or documents with the .txt or .doc extensions, ignoring everything else.
*.?	This example of an include filter matches only files or documents with a single-character extension. This example matches files such as hello.1 and hello.2, but not hello.doc or hello.html.
*/documentation/*,*/specs/*	This example of an include filter only matches on specific subdirectories of a file share or local drive called documentation and specs.

Syntax and examples for SQL Database scanning are in the SQL Database section. See "Configuring and running SQL database scans" on page 1268.

Syntax and examples for SharePoint scanning are in the SharePoint section.

See "Configuring and running SharePoint server scans" on page 1278.

Syntax and examples for Endpoint Discover scanning are in the Endpoint section.

See "Setting up and configuring Endpoint Discover" on page 1389.

See "Using environment variables in Endpoint Discover scans" on page 1395.

# Filtering Discover targets by item size

Use size filters to exclude items from the matching process that are based on their size.

Size filters are only available for files on file shares, Endpoint files, Lotus Notes documents, SharePoint items, and Exchange items.

You can configure other options for this target.

See "Network Discover scan target configuration options" on page 1191.

#### To exclude items based on item size

- 1 In the Enforce Server administration console, go to **Manage > Discover** Scanning > Discover Targets.
- 2 Click the name of the scan that you want to filter based on item size.
- Click the Filters tab. 3
- Enter optional values under the item size filters.

Symantec Data Loss Prevention includes only the items that match your specified size filters. If you leave this field empty, Symantec Data Loss Prevention performs matching on items of all sizes.

Note that all filters are combined with "and" if a value is provided. Consider all filter values (for example include, exclude, and date) when adding or modifying scan filters. Avoid unintentionally including everything, or excluding everything from the scan.

- To exclude items smaller than a particular size, enter a number in the field next to **Ignore Smaller Than**. Then select the appropriate unit of measure (Bytes, KB, or MB) from the drop-down list next to it.
- To exclude items larger than a particular size, enter a number in the field next to **Ignore Larger Than**. Then select the appropriate unit of measure (Bytes, KB, or MB) from the drop-down list next to it.
- 7 Click **Save** to save all updates to this target.

## Filtering Discover targets by date last accessed or modified

Specify date filters to exclude items from the matching process based on their dates. Only the items that match the specified date filters are included.

Date Filters are available for files on file shares, Endpoint files, Lotus Notes documents, and Microsoft SharePoint and Exchange documents.

Incremental scanning and differential scanning are available for some Network Discover target types.

See "Scanning new or modified items with incremental scans" on page 1224.

See "Scanning new or modified items with differential scans" on page 1225.

You can configure other options for this target.

See "Network Discover scan target configuration options" on page 1191.

Note that all filters are combined with "and" if a value is provided. Consider all filter values (for example include, exclude, and size) when adding or modifying scan filters. Avoid unintentionally including everything, or excluding everything from the scan.

To exclude items based on the date last accessed or modified

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click the Filters tab.
- 3 Enter optional values under File Date Filters.

Select Only Scan files added or modified since the last full scan for a differential scan.

See "Scanning new or modified items with differential scans" on page 1225.

This option scans only the items that have been added or modified (whichever is newer) since the last full scan.

If you do not select this option, Symantec Data Loss Prevention uses no date filter. It performs matching on items of all dates in the specified target.

The first scan has to be a full scan. A full scan occurs if you select this option before Symantec Data Loss Prevention scans this target for the first time.

When you select this option, you can also select the option Make next scan a full scan. When you select this option, the date filters for Only scan files added or modified and for Only scan files last accessed are disabled. The next scan is a full scan (if no previous full scans have completed). Subsequent scans cover only those items that have been added or modified since the full scan. After Symantec Data Loss Prevention performs the full scan, this check box is automatically deselected.

This option is not available for the target for a file system (file share). Use incremental scanning, instead.

See "About incremental scans" on page 1223.

See "About the difference between incremental scans and differential scans" on page 1222.

Select Only scan files added or modified to include files based on the added 5 or modified date.

Symantec Data Loss Prevention only scans items after the specified After date, before the specified **Before** date, or between the dates you specify.

Note that if the **After** date is later than the **Before** date, then no items are scanned. If the **Before** date and the **After** date are the same, then no items are scanned. No items are scanned because the assumed time of the Before parameter is at zero hours, and After is at 24 hours.

When you select this option, you can also select from the following options:

#### After

To include the items that are created or modified (whichever is newer) after a particular date, type the date. You can also click the date widget and select a date.

#### Before

To include the items that are created or modified (whichever is older) before a particular date, type the date. You can also click the date widget and select a date.

Select **Only scan files last accessed** to include files based on the last accessed date.

Symantec Data Loss Prevention only scans items after the specified After date, before the specified **Before** date, or between the dates you specify.

The last-accessed feature is only supported for Windows Network Discover Server scanning of CIFS shares.

Note that if the **After** date is later than the **Before** date, then no items are scanned. If the Before date and After date are the same, then no items are scanned. No items are scanned because the assumed time of the Before parameter is at zero hours, and After is at 24 hours.

When you select this option, you can also select from the following options:

#### After

To include the items that are accessed after a particular date, enter the date. You can also click the date widget and select a date.

#### Before

To include the items that are accessed before a particular date, enter the date. You can also click the date widget and select a date.

Note: The default mount process uses the CIFS client. If the default mount does not work, the mount task can use the java-based CIFS client by setting filesystemcrawler.use.jcifs=true in the properties file Crawler.properties.

Click **Save** to save all updates to this target.

# Optimizing resources with Network Discover scan throttling

You can set throttling options on the **Advanced** tab of the target for the following scan targets:

- File shares
- Endpoint files
- Lotus Notes documents
- SQL Databases

For the scanners, throttling must be set by editing the configuration file on the scanner computer.

Note: Use of item throttling significantly reduces the scan rate. Expect the scan rate to reduce to half the original scan rate or less.

You can also set other options to optimize scans.

See "About Network Discover scan optimization" on page 1220.

To set scan throttling for file shares, Lotus Notes documents, or SQL Databases

- In the Enforce Server administration console, go to **Manage > Discover** Scanning > Discover Targets.
- 2 Click the scan target name to open the target for editing.
- 3 On the **Advanced** tab, set the throttling options.
- Enter the maximum number of files or rows to be processed per minute, or the maximum number of bytes to be processed per minute.

If you select both options, then the scan rate is slower than both options.

File Throttling Specify the maximum number of files,

documents (in Lotus Notes), or rows (in

SQL Databases) to be processed per

minute.

Byte Throttling Specify the maximum number of bytes to

be processed per minute.

Specify the unit of measurement from the drop-down list. The options are bytes, KB

(kilobytes), or MB (megabytes).

### To set item throttling for the scanners

- Locate the scanner configuration file (scanner-type.cfg) on the computer where the scanner was installed.
- 2 In the scanner configuration file, modify the ImportPoliteness parameter and the BatchSize parameter.
  - When you set item throttling, the scanner fetches BatchSize items to local storage and then waits for ImportPoliteness milliseconds between processing each item fetched.
  - Byte throttling is not supported for any of the scanners.
- 3 To achieve item throttling from the repository, make the BatchSize parameter a small value. Then the ImportPoliteness value has more effect. Setting BatchSize=1 achieves the most throttling in fetching the documents.
  - For example, if you set BatchSize=25, and ImportPoliteness=5000 (5 seconds), the scanner downloads the 25 documents. Then it pauses 5 seconds between processing each document.

## Creating an inventory of the locations of unprotected sensitive data

To audit whether confidential data exists on a target, without scanning all of it, use Inventory Mode scanning. Inventory Mode is useful when the existence of incidents is important, not the number of them in each location.

Running a scan in Inventory Mode can also improve the performance of scanning large numbers of computers or large amounts of data. Setting incident thresholds can improve the performance of scanning by skipping to the next content root to scan, rather than scanning everything. A content root is one line (a file share, Domino server, or SQL database) specified on the **Scanned Content** tab.

You can set a maximum number of incidents for a scan item. The scan item can be a file share or a physical computer.

After the incident threshold has been reached, the scanning of this content root is stopped, and scanning proceeds to the next content root. Because the process is asynchronous, a few more incidents may be created than specified in the incident threshold.

Inventory Mode scanning is supported for the following server-based scan targets:

File shares

For file shares, you can also specify whether to count incidents by content root, or by computer. The content root is one file share on the list that is specified on the Scanned Content tab. The selection is specified in the field Count

Lotus Notes databases

Incidents Bv.

The incident threshold is counted per content root (Domino server from the list on the Scanned Content tab).

SQL databases

The incident threshold is counted per content root (SQL database from the list on the Scanned Content tab).

Inventory Mode can be set with the incident threshold parameter. You can set it when you add a new target, or when you edit an existing target.

After you locate the sensitive data, you can set other options to run the complete scans that target those locations.

See "Network Discover scan target configuration options" on page 1191.

## To create an inventory of sensitive data

- 1 In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click the scan target name to open the target for editing.
- 3 On the **Advanced** tab, you can optimize scanning with Inventory Mode scanning.
- 4 Set the Incident Threshold.

Enter the number of incidents to produce before moving on to the next content root (specified on the **Scanned Content** tab).

5 Set the **Count Incidents By** option.

For file shares you can also choose the following methods to count the incidents:

Content root (the default)

The content root is one file share from the list on the **Scanned Content** tab.

After the incident threshold is reached, the scan moves to the next file share.

#### Machine

Select this option to count by computer (from the specified shares on a computer).

When the incident threshold is reached, the scan moves to the next content root on the list to scan. If that content root is on the same physical computer as the previous item, it is skipped.

Note that the computer name must be literally the same, for the content root to be skipped. For example, \\localhost\myfiles and

\\127.0.0.1\myfiles are treated as different computers, even though they are logically the same.

# Chapter

# Managing Network Discover target scans

This chapter includes the following topics:

- Managing Network Discover target scans
- Managing Network Discover Targets
- Managing Network Discover scan histories
- Managing Network Discover Servers
- About Network Discover scan optimization
- About the difference between incremental scans and differential scans
- About incremental scans
- Scanning new or modified items with incremental scans
- About managing incremental scans
- Scanning new or modified items with differential scans
- Configuring parallel scanning of Network Discover targets

## Managing Network Discover target scans

Management tasks for your Network Discover target scans fall into four broad categories: managing Network Discover targets, managing Network Discover scan histories, managing Network Discover servers, and optimizing scans.

See "Managing Network Discover Targets" on page 1210.

See "Managing Network Discover scan histories" on page 1212.

See "Managing Network Discover Servers" on page 1219.

See "About Network Discover scan optimization" on page 1220.

# Managing Network Discover Targets

To manage your Discover scan targets, you can:

- Start, stop, and pause target scans.
- Monitor status as target scans run.
- Select targets to view details about them.
- Edit or delete targets.
- Manage multiple targets.
- Sort and filter targets for easier target management.
- Specify the number of targets to display.

See "About the Network Discover scan target list" on page 1210.

See "Working with Network Discover scan targets" on page 1211.

See "Removing Network Discover scan targets" on page 1212.

## About the Network Discover scan target list

You can manage your Network Discover scan targets on the Discover Targets screen. The toolbar above the target list includes a drop-down menu for creating new scan targets; buttons for starting, stopping, and pausing scans; and an icon for filtering the items in the list. You can apply actions to multiple targets.

You can click most column headers to sort the list by the data in that column.

You can select the number of entries to display in the **Discover Target** list using the drop-down menu above the **Actions** column.

See "Managing Network Discover target scans" on page 1209.

Table 57-1 lists the columns for each target scan.

Table 57-1 **Discover Targets** 

Target Information	Description
Target Name	Name of the target scan.
Target Type	Type of target for the scan (such as File System or SharePoint).

Target Information	Description
Policy Groups	Lists the policy groups to which the target is assigned.
Servers	Lists the servers assigned to this target.
Last Modified	Specifies the date and time that the target was last modified.
Scan Status	Displays the status of the scan. Click the link in this column to view a filtered scan history page for this target.
Next Scan	Displays the next scheduled scan for the target, if applicable.
Actions	Click the <b>Edit Target</b> icon to edit the target definition.
	Click the <b>Delete</b> icon to delete the target.

Table 57-1 Discover Targets (continued)

## To filter the Discover Target list

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click Filter. A text field or drop-down list appears in each column header in the Discover Target list.
- 3 Apply one of these filters to the list:
  - **Target Name**: Type the name of the target into the text field.
  - Target Type: Select the target type from the drop-down list.
  - Policy Groups: Type the name of the policy group into the text field.
  - **Servers**: Type the name of the server into the text field.
  - Last Modified: Select a range from the drop-down list.
  - Scan Status: Select a scan status from the drop-down list.
  - Next Scan: Select a range from the drop-down list.
- To clear a filter, clear the value from the relevant text field or drop-down list, or click Filter.

## Working with Network Discover scan targets

You can perform the following tasks with your scan targets:

## To start, stop, and pause Network Discover scans

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Select the scan target or targets you want to start, stop, or pause.
- Click the **Start**, **Stop**, or **Pause** button on the target list toolbar.

### To edit a Network Discover scan target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click the **Edit Target** button for the target you want to edit.
- Make your desired changes on the **Edit Target** page. See "Network Discover scan target configuration options" on page 1191.

## Removing Network Discover scan targets

Check the scans that are running or queued before removing a scan target.

See "Managing Network Discover target scans" on page 1209.

To remove scan targets, perform these actions:

- Remove the scan target from the Enforce Server.
- Uninstall the scanner from the computer where it is installed, if applicable.

#### To remove a scan target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click **Delete** icon for the target you want to remove.

## Managing Network Discover scan histories

To manage your Network Discover scan histories, you can:

- View statistics about running or completed scans.
- Download scan history information in comma-separated value (CSV) format.
- View scan details.
- View incident reports.
- Delete scan histories.
- Manage multiple scan histories.

- Sort and filter scan histories for easier management.
- Specify the number of scan histories to display.

See "About Network Discover scan histories" on page 1213.

See "Working with Network Discover scan histories" on page 1214.

See "Deleting Network Discover scans" on page 1215.

See "About Network Discover scan details" on page 1215.

See "Working with Network Discover scan details" on page 1218.

## About Network Discover scan histories

You can manage your Network Discover scan histories on the Scan History screen. To view a scan history list for all Discover targets, in the Enforce Server administrative console, go to Manage > Discover Scanning > Scan History.

You can click any column header to sort the list alpha-numerically by the data in that column.

You can select the number of entries to display in the Discover Target list using the drop-down menu above the Actions column.

For more details about a scan, click the link in the Scan Status column to display the Scan Detail screen.

See "About Network Discover scan details" on page 1215.

See "Managing Network Discover target scans" on page 1209.

Table 57-2 lists the fields that are displayed for each scan.

**Table 57-2** Scan History

Scan History	Description
Target Name	Name of the target scan.
Target Type	Type of target for the scan (such as File System or SharePoint).
Scan Started	Date and time the scan started.
Scan Status	Current status of the scan: Running, Paused, Completed, Stopped.
Scan Type	Scan type: Incremental, Differential, or Full.

Scan History	Description
Incident Count	Number of incidents found in the scan.
Run Time	Elapsed time of the scan in dd:hh:mm:ss format.
Bytes/Items Scanned	Number of bytes scanned in the target, as well as the number of items scanned.
Errors	Number of errors during the scan.
Actions	Click the View Incidents icon to view an incident summary report for the scan.  See "About incident reports for Network Discover" on page 989.  See "Discover incident reports" on page 990.  Click the Delete icon to delete the scan. Make sure to first delete differential scans before you delete the base scan.  See "Deleting Network Discover scans" on page 1215.

Table 57-2 Scan History (continued)

### To filter the Scan History list

- In the Enforce Server administration console, go to Manage > Discover Scanning > Scan History.
- 2 Click Filter. A text field or drop-down list appears in the column header in the Scan History list.
- 3 Apply one of these filters to the list:
  - **Target Name**: Type the name of the target into the text field.
  - **Target Type**: Select the target type from the drop-down list.
  - Scan Started: Select a range from the drop-down list.
  - Scan Status: Select a scan status from the drop-down list.
  - Scan Type: Select a scan type from the drop-down list.
- To clear a filter, clear the value from the relevant text field or drop-down list, or click Filter.

## Working with Network Discover scan histories

You can perform the following tasks with your scan histories:

### To export Network Discover scan histories

- In the Enforce Server administration console, go to Manage > Discover Scanning > Scan History.
- 2 Select the scan or scans you want to export.
- 3 Click **Export**. The File Download dialog box appears.
- 4 Click **Open** to view the exported data, or click **Save** to save the file.
- 5 To cancel the export operation, click **Cancel**.

## To view incidents for a specific scan

- In the Enforce Server administration console, go to Manage > Discover Scanning > Scan History.
- 2 Click the View Incidents icon for the scan you want to view. The Discover **Incidents** screen appears.

## **Deleting Network Discover scans**

You can delete specific scans from your scan history.

#### To delete a scan

- In the Enforce Server administration console, go to Manage > Discover Scanning > Scan History.
- 2 Delete any differential scans before you delete the base full scan for that target. This step is not necessary for incremental scans.
- 3 Select the scan to be deleted, then click the delete icon in the **Actions** column. To delete multiple scans, mark the checkboxes for the scans you want to delete. then click **Delete** on the toolbar.

## About Network Discover scan details

You can view detailed information about each Network Discover scan, including general scan information, scan statistics, recent errors, and scan activity. You can also download reports in CSV format for scan statistics, recent errors, and scan activity.

To view scan details, go to Manage > Discover Scanning > Scan History. Select the scan, then click the link in the Status column.

See "Managing Network Discover target scans" on page 1209.

Table 57-3 shows the General section which displays information about the scan.

**Table 57-3** General Scan Detail

General Scan Detail	Description
Target Type	The type and icon of the target that was scanned.
Target Name	Name of the target.
Status	Status of the scan.  If the scan is running, the name of the Network Discover Server where this scan is running is displayed.
Scan Type	Scan type, such as incremental or full.
Start Time	The date and time the scan began.
End Time	The date and time the scan finished.

Table 57-4 shows the Scan Statistics section, which provides detailed information about the scan.

Scan Statistics **Table 57-4** 

Scan Statistics	Description
Processed	Number of items that have been scanned. If the scan is still running, this field provides a benchmark of scan progress.
Run Time (dd:hh:mm:ss)	Amount of time that the scan took to complete. If the scan is still running, the amount of time that it has been running. The total does not include any time during which the scan was paused.
Items Scanned	Number of items scanned.
Bytes Scanned	Number of bytes scanned.
Errors	Number of errors that occurred during the scan. A list of the errors is available in the <b>Recent Scan Errors</b> section.

Scan Statistics	Description
Total Detected Incident Count	Total number of incidents that were detected during the current scan.
Current Incident Count	Number of incidents that were detected during the current scan, less any deleted incidents. You can click this number to see an incident list for this scan.

**Table 57-4** Scan Statistics (continued)

The Recent Scan Errors section is a listing of the errors that occurred during the scan.

If a scan has many errors, the Scan Detail screen does not display them all. To see a complete list of errors that occurred during the scan, click Download Full Error Report.

Table 57-5 shows the information in the Recent Scan Errors report, which provides information about each error.

Recent Scan Errors **Table 57-5** 

Recent Scan Error Details	Description
Date	The date and time of the error during the scan.
Path	The directory path to the location of the file with the error during the scan.
Error	The error message.

Recent Scan Activity displays the most recent log entries of the notable events that occurred during the scan.

If a scan has many activity messages, the Scan Detail screen does not display them all. To see a complete list of scan activity messages, click Download Full **Activity Report.** 

Table 57-6 shows the Recent Scan Activity report, which provides information about each activity.

Table 37-0	Recent Scan Activity
Recent Scan	Description
Activity	

Recent Scan Activity

Details Date/Time The date and time when the logged event occurred. Level The severity of the event. Message The message that was logged about the event.

Table 57-7 explains the options on the Scan Detail screen.

**Table 57-7** Options on the Scan Detail screen

Scan Detail options	Description
Download Full Statistics Report	Download a report with all scan statistics in CSV format.
Download Full Error Report	Download a report with all scan errors in CSV format.
Download Full Activity Report	Download a report with all scan activity in CSV format.

## Working with Network Discover scan details

Table 57-6

You can perform the following tasks with scan details:

#### To view scan details

- In the Enforce Server administration console, click Manage > Discover Scanning > Scan History.
- 2 On the Scan History page, click the link in the Scan Status column for the scan for which you want to view details.

## To export scan details to a CSV file

- In the Enforce Server administration console, go to Manage > Discover Scanning > Scan History.
- 2 On the Scan History page, click the link in the Scan Status column for the scan for which you want to view details.
- 3 On the **Scan Details** page, click one of the following buttons:

- Download Full Statistics Report
- Download Full Error Report
- Download Full Activity Report

# **Managing Network Discover Servers**

You can view the status and scan details of Network Discover scans for each Discover server.

See "Viewing Network Discover server status" on page 1219.

## Viewing Network Discover server status

The Discover Servers screen lists the detection servers for Network Discover or Endpoint Discover that are configured on your network. This screen shows details about the scans on each detection server.

To view your Discover servers, in the Enforce Server administration console, go to Manage > Discover Scanning > Discover Servers.

See "Managing Network Discover target scans" on page 1209.

Table 57-8 lists the information for each server.

Discover Servers Table 57-8

Server Information	Description
Server Name	The name of the server. In parentheses is the type of detection server, either Discover or Endpoint.
Running Scans	A list of the scans that are currently running on this server.
Queued Scans	A list of the scans that are queued to run on this server.
Scheduled Scans	A list of scans that are scheduled to run in the future on this server.
Paused Scans	A list of the paused scans on this server.

#### To view scan details from a Network Discover server

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Servers
- 2 On the **Discover Servers** page, click the name of the scan for which you want to view details.

See "About Network Discover scan details" on page 1215.

## About Network Discover scan optimization

Network Discover Target scans can take hours or days to complete, depending on the type of scan and the amount and format of the data to be scanned, as well as hardware and network speed. To optimize your scans of large amounts of information for better performance, follow the suggestions in this section.

To help optimize your Network Discover scans, consider using some of the following methods:

- Begin by scanning only the file shares or repositories that are the most accessed and most widely available (for example, quest or public access). Start small, and confirm the accuracy of your scans before increasing the volume of information in a scan. After you have achieved satisfactory performance with your initial scans, add scanning for the business units that handle your confidential data.
- Install multiple Network Discover Servers on the network.
- Break large scans into multiple smaller scans. Create separate scan targets and use filters to break up the set to scan.

You can break up scans with include, exclude, size, and date filters. See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

See "Filtering Discover targets by item size" on page 1201. See "Filtering Discover targets by date last accessed or modified" on page 1202.

Scan non-binary files first. Binary files are less likely to contain policy violations. For example, you can set the Exclude Filter to the following list to scan non-binary files:

```
*.exe, *.lib, *.bin, *.dll, *.cab, *.dat
*.au, *.avi, *.mid, *.mov, *.mp, *.mp3, *.mp4, *.mpeg, *.wav, *.wma
```

To scan the rest of the files, use this filter as the Include Filter of a different scan

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

For File System targets, you can configure incremental scans to check only those files that have not yet been scanned.

See "Scanning new or modified items with incremental scans" on page 1224. See "About the difference between incremental scans and differential scans" on page 1222.

 Scan new or recently modified items in one scan target, and older ones in a second scan target.

Use the date filter to break up scans by date values, by files older than, or files newer than.

See "Filtering Discover targets by date last accessed or modified" on page 1202.

 After the initial scan, run differential scans to check only those items that were added or modified since the last complete scan.

See "Scanning new or modified items with differential scans" on page 1225. See "About the difference between incremental scans and differential scans" on page 1222.

 Scan small files in one scan target and large files in another. Scanning many small files carries more overhead than fewer large files. Use the size filter to break up scans by size.

See "Filtering Discover targets by item size" on page 1201.

 Scan compressed files in a separate scan target. Use the Include Filter to scan compressed files. For example, use the following list:

```
*.zip, *.gzip
```

To scan the rest of the files, use this filter as the Exclude Filter of a different scan target.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

Scan database or spreadsheet files in a separate scan target.

Use the SQL Database target to scan database files.

See "Configuring and running SQL database scans" on page 1268.

Use the Include filter to scan spreadsheet files:

```
*.xls
```

Set up a separate scan target and use the Exclude Filter to scan everything else.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

 Exclude the folders internal to applications. For example, in the scan of a DFS share, exclude the internal DfsrPrivate folder. In the scan of a share on a NetApp filer, exclude the .snapshot folder.

See "Excluding internal DFS folders" on page 1253.

See "Configuring and running scans of file systems" on page 1254.

- Use Inventory Mode scanning to move to the next scan item after an incident threshold is reached. Inventory Mode scanning can audit where confidential data is stored without scanning all of it.
  - See "Creating an inventory of the locations of unprotected sensitive data" on page 1206.
- Dedicate as much hardware as possible to the scans. For example, suspend or quit any other programs that run on the server.
- Use Scan Pausing to automatically suspend scanning during work hours.
- Run scans in parallel. See "Configuring parallel scanning of Network Discover targets" on page 1226.
- Use throttling to reduce network load. See "Optimizing resources with Network Discover scan throttling" on page 1204.
- Update the server hardware. You can use up to 12 GB of memory, quad CPUs, ultra-fast hard drives, and network cards to address any bottlenecks in the hardware.

## About the difference between incremental scans and differential scans

Incremental and differential scans let you optimize scan performance by scanning only new or modified items. Incremental scans resume from whatever point they left off, whether or not the first scan was a full scan. Differential scans only scan items added or modified after the last full scan: you must run at least one full scan on your scan target before you can use differential scanning.

See "About incremental scans" on page 1223.

See "Scanning new or modified items with incremental scans" on page 1224.

See "Scanning new or modified items with differential scans" on page 1225.

Table 57-9 compares incremental scans and differential scans.

Table 57-9 Differences between incremental scans and differential scans

Incremental scans	Differential scans
Incremental scans are supported for the following targets:  Server > File System Server > SharePoint	Differential scans are supported for the following targets:  Server > Lotus Notes Server > Exchange Endpoint > File System

**Table 57-9** Differences between incremental scans and differential scans (continued)

Incremental scans	Differential scans
Partial scans retain the information about the items that have been scanned.  If files, shares, or other items are missed because they are inaccessible, the next incremental scan automatically covers the missed items.	Differential scans begin with a full scan of the Discover target. This full scan is called the base scan. Partial scans cannot be used as a base scan.
Subsequent runs scan all items that have not previously been scanned, including new or modified items.	Subsequent runs scan all items that have been added or modified since the date of the most recent full (base) scan completed.  The system considers the start date of the base scan for differential scanning.
An incremental scan index keeps track of which items have already been scanned.	The most recent complete base scan serves as the comparison for which items to scan, based on the date of the base scan.

## About incremental scans

Incremental scans let you optimize scan performance by scanning only new or modified items. Incremental scans resume from whatever point they left off, whether or not the first scan was a full scan

See "About Network Discover scan optimization" on page 1220.

Incremental scanning is only supported for some targets types.

See "About the difference between incremental scans and differential scans" on page 1222.

Incremental scans retain the information about the items that have been scanned.

Some files may be skipped during a scan, for example, because they are locked or in use. A scan may not complete because the data cannot be accessed, such as when a server or device is offline. These missed files are scanned during subsequent scans of this target.

An incremental scan index keeps track of which items have been scanned previously. This index is synchronized between multiple Discover Servers.

For information about sizing requirements for the incremental scan index, see the Symantec Data Loss Prevention System Requirements and Compatibility Guide.

## Scanning new or modified items with incremental scans

An incremental scan lets you resume a Network Discover scan from where you left off. An incremental scan only scans the items that have not been scanned previously.

See "About the difference between incremental scans and differential scans" on page 1222.

## To set up an incremental scan

- Go to Manage > Discover Scanning > Discover Targets.
- 2 Click the drop-down New Target, and select the File System or SharePoint target type, or select one of the file system or SharePoint scan targets in the list to edit it.
- 3 Click the General tab.
- Under Scan Type, select Scan only new or modified items (incremental **scan)**. This option is the default for new targets.

If you have changed the policy or other definitions in an existing scan, you may want to set up the next scan as a full scan to ensure complete policy coverage. Select the following option:

Scan all items for the next scan. Subsequent scans will be incremental.

If you always want to scan all items in this target, select the following option:

#### Always scan all items (full scan)

5 Complete the other steps to set up or modify a Discover target and run the scan.

See "Configuring the required fields for Network Discover targets" on page 1193.

See "Network Discover scan target configuration options" on page 1191.

See "Setting up server scans of file systems" on page 1241.

To manage incremental scanning and diagnose issues, refer to the following topic:

See "About managing incremental scans" on page 1225.

# About managing incremental scans

Note the following when running incremental scans:

- If your installation has multiple Discover Servers, the incremental scan index is automatically synchronized to all the other Discover Servers for that target.
- When you change the incremental scan setting from Scan only new or modified items (incremental scan) to Scan all items for the next scan. Subsequent scans will be incremental, then the incremental scan index for that target is cleared before the scan starts. Subsequent scans are incremental.
- To scan all items, set Always scan all items (full scan) for the Discover target.
- If the setting Always scan all items (full scan) is selected, then any previous index entries for that target are cleared before the scan starts. The index is not repopulated during the scan.
  - If you want to scan all items and then continue incremental scanning, select the option Scan all items for the next scan. Subsequent scans will be incremental.
- When a Discover target is deleted, the incremental scan index is not automatically

# Scanning new or modified items with differential scans

To save resources, differential scans only scan the items that have been added or modified since the last full scan.

For information about how a target that is configured for differential scanning is upgraded during a version upgrade, see the Symantec Data Loss Prevention Upgrade Guide.

See "About the difference between incremental scans and differential scans" on page 1222.

### To set up a differential scan

- 1 Go to Manage > Discover Scanning > Discover Targets.
- Click the drop-down New Target, and select the target type, or select one of 2 the scan targets in the list to edit it.
- 3 Click the **Filters** tab.
- Select the date option for a differential scan.
  - See "Filtering Discover targets by date last accessed or modified" on page 1202.

- 5 Run a full scan. The initial scan must be a full scan.
- 6 After the initial scan has completed, the next scan only scans the items that are added or modified since the last full scan.

# Configuring parallel scanning of Network Discover targets

Multiple scans of different targets can be run simultaneously on the same Network Discover Server.

Parallel scans of server and scanner target types are supported. Parallel scanning of Endpoint file systems is not supported. Parallel scanning of the same CIFS server or share with different credentials, and from the same Network Discover Server is not supported.

The scan can be controlled (paused, resumed, or stopped) independent of other scans that are on the Network Discover Server. The state of each scan is maintained and reported separately.

When a scan is started and multiple Network Discover Servers are selected, one is selected for this scan. The scan is assigned to run on the server with the fewest number of scans that are running. The server is chosen from the server set specified in the target.

After a scan starts, it continues to run on the same server until the scan completes, is aborted, or paused. On resumption the scan may be assigned to run on a different server.

Automated load balancing is not supported. If a Network Discover Server completes running all its scans, scans from other servers do not migrate to the unloaded server. However, a scan can be migrated manually, by pausing and restarting the scan.

To run multiple scanner targets on the same Network Discover Server, separate ports must be configured for each scanner. The default port for a new scanner is a value not already used by any scan targets.

See "Troubleshooting scanners" on page 1307.

### To configure parallel scanning

- In the Enforce Server administration console, go to System > Servers > Overview.
- 2 Select a Network Discover Server to configure, and click the server name.
- 3 Click the **Configure** option at the top.
- 4 Then select the **Discover** tab.

- 5 Set the maximum number of parallel scans to run on this Network Discover Server.
  - The default value for **Maximum Parallel Scans** is 1. The maximum count can be increased at any time. After it is increased, then any gueued scans that are eligible to run on the Network Discover Server are started. The count can be decreased only if the Network Discover Server has no running scans. Before you reduce the count, pause or stop all scans on the Network Discover Server.
- Click Save. 6
- 7 Click Done.
- You can view the scans that are actively running, queued, scheduled, or paused on each Network Discover Server. In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Servers.
  - See "Managing Network Discover target scans" on page 1209.

# Using Server FlexResponse plug-ins to remediate

incidents

This chapter includes the following topics:

- About the Server FlexResponse platform
- Using Server FlexResponse custom plug-ins to remediate incidents
- Deploying a Server FlexResponse plug-in
- Locating incidents for manual remediation
- Using the action of a Server FlexResponse plug-in to remediate an incident manually
- Verifying the results of an incident response action
- Troubleshooting a Server FlexResponse plug-in

# About the Server FlexResponse platform

The Server FlexResponse application programming interface (API) provides a flexible platform for incident remediation. It enables Symantec Data Loss Prevention users to protect data by automatically or manually invoking custom Server FlexResponse actions.

Symantec provides a set of Server FlexResponse plug-ins that perform various remediations such as quarantining sensitive data, copying files, and applying digital rights protection or encryption. Independent developers can also write Server FlexResponse plug-ins to perform custom incident remediation using this API and

the Java programming language. The Server FlexResponse API enables developers to build a plug-in that can be used to implement incident responses for use in Automated and Smart Response rules.

The following are example Network Protect actions that you can implement by developing a Server FlexResponse plug-in:

- Change Access Control Lists (ACL) on files. For example, you can remove guest access to selected files.
- Apply Digital Rights Management (DRM). For example, you can apply digital rights to documents so external parties are restricted in their access to sensitive material. These digital rights can include "do not forward" or "do not print."
- Encrypt files.
- Migrate files to SharePoint. The custom protect action can move files from shares to a SharePoint repository, and then apply DRM and ACLs.
- Perform workflow and automation of remediation responses.
- Use the Symantec Workflow business process automation workflow.

The following steps are involved in building, deploying, and using a Server FlexResponse plug-in:

- Developing a plug-in using the Java API. This stage involves designing and coding the plug-in and remediation action.
- Configuring plug-in parameters by creating the configuration properties file for your plug-in.
  - See "Creating a properties file to configure a Server FlexResponse plug-in" on page 1233.
- Adding your plug-ins to the plug-ins configuration properties file. See "Adding a Server FlexResponse plug-in to the plug-ins properties file" on page 1232.
- Deploying your custom plug-in on the Enforce Server. See "Deploying a Server FlexResponse plug-in" on page 1231.
- Loading the plug-in, including the plug-in metadata.
- Creating response rules for incident Smart Response actions.
- Using the plug-in action to remediate an incident. See "Using the action of a Server FlexResponse plug-in to remediate an incident manually" on page 1237.
- Verifying the results of the Server FlexResponse plug-in action. See "Verifying the results of an incident response action" on page 1238.

Note: Server FlexResponse plug-ins that were created for Symantec Data Loss Prevention versions 10 and 11 are compatible with Symantec Data Loss Prevention version 12.

The sections that follow describe how to deploy and configure pre-made FlexResponse plug-ins, as well as how to use custom plug-in actions in Symantec Data Loss Prevention policies. You can obtain some Server FlexResponse plug-ins directly from Symantec. You can also develop your own custom plug-ins using the Server FlexResponse API. For information about developing plug-ins using the Java API, See the Symantec Data Loss Prevention Server FlexResponse Platform Developers Guide.

# Using Server FlexResponse custom plug-ins to remediate incidents

You can use Server FlexResponse plug-in actions to automatically or manually remediate Network Discover incidents.

To develop a custom remediation action, see the Symantec Data Loss Prevention Server FlexResponse Platform Developers Guide.

To automatically or manually remediate incidents with a custom Server FlexResponse plug-in, you must perform the following steps:

**Table 58-1** 

Step	Action	Description
1	Deploy a Server FlexResponse plug-in to the Enforce Server computer.	Each Server FlexResponse plug-in must be deployed to the Enforce Server computer before you can use the plug-in actions in Symantec Data Loss Prevention policies.  See "Deploying a Server FlexResponse plug-in"
		on page 1231.
2	Create a response rule that uses a custom Server FlexResponse incident response action.	See "Configuring the Server FlexResponse action" on page 912.

Step Description Action 3 (Optional) Use the Server FlexResponse If you are using a Server FlexResponse plug-in action in a plug-in to manually remediate incidents. smart response rule, you must manually locate an incident and execute the FlexResponse action. See "Locating incidents for manual remediation" on page 1236. See "Using the action of a Server FlexResponse plug-in to remediate an incident manually" on page 1237. This step is not necessary if you configure an automated response rule to execute a Server FlexResponse action. With automated response rules, the creation of an incident that triggers the automated response rule also executes the configured FlexResponse action. 4 Verify the results. See "Verifying the results of an incident response action" on page 1238.

Table 58-1 (continued)

# Deploying a Server FlexResponse plug-in

Enable a plug-in for the Server FlexResponse API.

### To deploy a Server FlexResponse plug-in

Copy the completed Server FlexResponse plug-in JAR file to the plug-ins directory:

SymantecDLP\Protect\plugins\

- 2 Configure the plug-in with a properties file.
  - See "Creating a properties file to configure a Server FlexResponse plug-in" on page 1233.
- Copy the properties file for each plug-in into the directory where you placed your JAR file:

SymantecDLP\Protect\plugins\

- In the file SymantecDLP\Protect\config\Plugins.properties, add the plug-in to the list, and enter the properties for your plug-in.
  - See "Adding a Server FlexResponse plug-in to the plug-ins properties file" on page 1232.

- 5 Make sure that the Symantec Data Loss Prevention protect user has read and execute access to both the plug-in JAR file and the plug-in properties file.
- To load the plug-in, stop the Vontu Incident Persister and Vontu Manager services, and then restart them.

# Adding a Server FlexResponse plug-in to the plug-ins properties file

Add a Server FlexResponse plug-in to the Plugins.properties file. Also, modify any parameters that are necessary for the plug-in.

### To add a Server FlexResponse plug-in to the properties file

Edit the Plugins.properties file.

General values are in this file for all plug-ins, plus a list of all the plug-ins that are implemented.

See Table 58-2 on page 1233.

This file is in the following directory:

```
SymantecDLP\Protect\config
```

Locate the following line in the file, which specifies the JAR files of the plug-ins to construct at load time:

```
# Incident Response Action configuration parameters.
com.symantec.dlpx.flexresponse.Plugin.plugins =
```

Remove the comment mark from the beginning of the line, if necessary, and replace plugin1.jar, plugin2.jar with the names of the plug-in JAR files you want to deploy. Separate multiple JAR files with commas.

Edit any additional parameters in this file.

plugin1.jar,plugin2.jar

Table 58-2 describes the additional properties for the Server FlexResponse API in the Plugins.properties file.

Stop the Vontu Incident Persister and Vontu Manager services, and then restart them. This loads the new plug-in and the other parameters in this file.

If you later change the Plugins.properties file, you must restart both the Vontu Incident Persister and Vontu Manager services to apply the change.

In Table 58-2 plugin-id is a unique identifier of the plugin within this properties file, for example test1.

**Table 58-2** Parameters in the Plugins.properties file

Property name	Description
protect.plugins.directory	The directory under which all Symantec Data Loss Prevention plug-ins are installed.
com.symantec.dlpx.flexresponse.Plugin.plugins	A comma-separated list of JAR files (or JAR titles) to be loaded in the Server FlexResponse plug-in container.
	Each plug-in in this list will correspond to a response rule action in the Enforce Server administration console.
	The container in which your JAR file is deployed includes all of the public JRE classes provided by the JVM installed with Symantec Data Loss Prevention. The container also includes all of the FlexResponse API classes described in this document (classes in the com.symantec.dlpx package hierarchy). Your FlexResponse plug-in code may have dependencies on other JAR files that are not provided by the plug-in container. Place any external JAR files that you require in the \plugins directory of the Enforce Server where the FlexResponse plug-in is deployed. Then reference the JAR in this property.
com.vontu.enforce.incidentresponseaction. IncidentResponseActionInvocationService. maximum-incident-batch-size	The maximum number of incidents that can be selected from the incident list report for one Server FlexResponse Smart Response rule invocation.  The default is 100.
	In this release, the maximum value of this parameter cannot exceed 1000.
com.vontu.enforce.incidentresponseaction. IncidentResponseActionInvocationService.	Do not change the value of this parameter. This parameter is reserved for development and debugging.
keep-alive-time	Use the timeout property in the individual plug-in properties file to set the timeout for the execution threads for your plug-in.
com.vontu.enforce.incidentresponseaction. IncidentResponseActionInvocationService.	The execution thread timeout for the serial thread executor (global).  See the is-serialized property in the individual plug-in property
serial-timeout	file for details.

# Creating a properties file to configure a Server FlexResponse plug-in

Specific information and parameters for each Server FlexResponse plug-in are in the plug-in-name.properties file.

Each plug-in must have a separate properties file.

An individual plug-in properties file is not necessary if the plug-in satisfies the following conditions:

- Does not need custom properties.
- Provides the display name and the plug-in identifier in the implementation of the plug-in metadata class.
- Does not need a stored credential.

### To configure a Server FlexResponse plug-in

Create a text file that contains the properties for each Server FlexResponse plug-in.

Each JAR file has an optional associated properties file with the same base name as the JAR file. These files are located in the SymantecDLP\Protect\plugins directory.

For example, if you have a plugin1.jar file, you should create a plugin1.properties file.

2 In this file, enter the keys and values of all the parameters for the plug-in:

```
display-name=plugin 1
plugin-identifier=IncidentResponseAction1
```

To update the properties, you must stop the Vontu Manager and Vontu Incident Persister services, and then restart them to load in the new values.

See Table 58-3 on page 1235.

Make sure that the Symantec Data Loss Prevention protect user has read and execute access to the plug-in properties file.

Table 58-3 describes the properties in the pluq-in-name.properties file.

Parameters in the custom plug-in properties file **Table 58-3** 

Property name	Description
display-name	The name of this plug-in.
	This name is displayed in the <b>choose a plugin</b> drop-down menu when you select an <b>All: Server FlexResponse</b> action in a Smart Response rule or an automated response rule.
	A best practice is to define this property in the plug-in properties file.
	If you change the value of this name in the properties file after the plug-in is loaded, you must restart the Vontu Incident Persister and Vontu Manager services to load in the new name.
	Alternatively, this value can be specified in the metadata class.
	This value is mandatory and it must be specified in at least one place, either in the configuration properties file, or the plug-in metadata class.
	For international environments, this display name can be in the local language.
plugin-identifier	The identifier for this plug-in. This identifier should be unique for all Server FlexResponse plug-ins on this Enforce Server.
	A best practice is to define this property in the plug-in properties file.
	Alternatively, this value can be specified in the metadata class.
	This value is mandatory and it must be specified in at least one place, either in the configuration properties file, or the plug-in metadata class.
	If any response rule is assigned to this Server FlexResponse plug-in, do not change this identifier in your properties file.
credential-reference.credential	Specifies a reference to a named credential to authenticate access, for example to an inventory database. The value of this property must refer to a named credential that was defined on the Enforce Server. The credential-reference in the property name provides a method to differentiate between multiple credentials in the properties file.
	<pre>inventory-credential.credential= InventoryDB1</pre>
custom name	These optional custom parameters are required to pass information to your plug-in.
Example:	These parameters are passed to each invocation of the plug-in and can optionally
test1.value.1	be made available at the time this plug-in is constructed.
test1.value.2	

**Table 58-3** Parameters in the custom plug-in properties file (continued)

Property name	Description
timeout	Optional parameter with the timeout in milliseconds for the execution threads for this plug-in.
	The default is 60000 (one minute).
	If the timeout value is reached, the user interface shows the Server FlexResponse plug-in status as failed, and the incident history is updated with a timeout message.
	If you change the value of this property in the properties file after the plug-in is loaded, you must stop the Vontu Incident Persister and Vontu Manager services, and then restart them.
maximum-thread-count	Optional parameter with the number of parallel threads available for execution of this plug-in. This parameter is ignored if is-serialized is set.
	The default is 2.
	If you change the value of this property in the properties file after the plug-in is loaded, you must stop the Vontu Incident Persister and Vontu Manager services, and then restart them.
is-serialized	The value of this parameter can be true or false. Set this optional parameter to true if this plug-in execution must be serialized (one thread at a time). All serialized plug-ins share a single execution thread. If this parameter is set, then timeout and maximum-thread-count are ignored.
	The default is false.
	If you change the value of this property in the properties file after the plug-in is loaded, you must stop the Vontu Incident Persister and Vontu Manager services, and then restart them.

# Locating incidents for manual remediation

To manually execute the plug-in action configured in a Smart Response Rule, use the reports on the Enforce Server to select incidents for remediation.

### To locate incidents for manual remediation

- 1 Log on to the Enforce Server administration console.
- 2 Click Incidents > Discover.
- 3 Select an incident (or multiple incidents) for remediation. You can use the standard reports or report filters to narrow the list of incidents.
- You can select either a group of incidents, or one incident for remediation:

- From the list of incidents, check the box to the left of each incident to select that incident for remediation. You can select multiple incidents.
- From the list of incidents, select all incidents on this page by clicking the check box on the left of the report header.
- From the list of incidents, select all incidents in the report by clicking the **Select All** option on the upper-right side of the report.
- Click one incident to display the Incident Detail, and select that one incident for possible remediation.

After you have selected the incidents for remediation, you can manually remediate them.

See "Using the action of a Server FlexResponse plug-in to remediate an incident manually" on page 1237.

# Using the action of a Server FlexResponse plug-in to remediate an incident manually

After you have selected an incident, or group of incidents to remediate, you can invoke the action of a Smart Response rule. This action uses your custom Server FlexResponse plug-in to remediate the incidents manually.

### To remediate a single incident

Be familiar with the response rules that are available to manually remediate an incident.

Click Policies > Response Rules.

The **Conditions** column indicates which rules can be executed manually.

- 2 Select a single incident, and display the Incident Detail.
  - See "Locating incidents for manual remediation" on page 1236.
- In the **Incident Detail** screen above the incident number, your remediation options display. These options show the names of your response rules.
- Click a Server FlexResponse plug-in remediation button to perform the remediation action.

- View the remediation action. Click **OK**.
- Verify that the remediation is complete. Some remediation actions may take a long time, for example encryption of a large file. To see user interface updates, click the refresh icon in the upper-right corner of the report. Refresh the page until you see the green success or red failure icon in the incident details.

See "Verifying the results of an incident response action" on page 1238.

### To remediate a selected group of incidents

Select incidents from an incident list report. Check the box at the left of the selected incidents.

Alternatively, you can select all incidents on a page or on a report.

See "Locating incidents for manual remediation" on page 1236.

- 2 **Incident Actions** becomes a drop-down menu.
- From the Incident Actions drop-down menu, select Run Smart Response and then select your custom Server FlexResponse.
- View the remediation action. Click **OK**.
- 5 Verify that the remediation is complete. Some remediation actions may take a long time, particularly if several incidents were selected. To see user interface updates, click the refresh icon in the upper-right corner of the report. Refresh the page until you see the green success or red failure icon in the incident details.

See "Verifying the results of an incident response action" on page 1238.

# Verifying the results of an incident response action

You can verify that a remediation action has been completed by using the **History** tab of an incident.

To verify the results of an incident response action for a single incident

- Log on to the Enforce Server administration console. 1
- Click Incidents > Discover.
  - Look for the green success or red failure icons in the incident report.
- 3 For additional information about the results, click one incident to display the Incident Detail.

- Click the **History** tab.
- 5 View the remediation messages from your plug-in. A message that your plug-in was invoked, and another message with the success or failure should display. Other messages may also display, with the status result or remediation result.

### To verify the results of an incident response action for a group of incidents

- Log on to the Enforce Server administration console. 1
- 2 Click Incidents > Discover.
- 3 Use report filters and summaries to display the protect or prevent status of the incidents.

See "Viewing incidents" on page 1018.

Custom reports can also be created to show the protect or prevent status, or the values of custom attributes.

See "About custom reports and dashboards" on page 1019.

# Troubleshooting a Server FlexResponse plug-in

Table 58-4 has troubleshooting issues and suggestions for diagnosing Server FlexResponse problems.

Troubleshooting suggestions **Table 58-4** 

Issue	Suggestions
During creation of a Smart Response Rule, the drop-down menu does not display the action All: Server FlexResponse.  During creation of an automated Response Rule, the drop-down menu.	This issue happens because your plug-in did not load.  At the end of the file Plugins.properties, enter the name of your plug-in JAR file on the list of plug-ins. Make sure that this line is not commented out.
does not display the action All: Server FlexResponse.  If you have multiple plug-ins, your plug-in name does not display in the All: Server FlexResponse drop-down	Restart both the Vontu Incident Persister and Vontu Manager services to load your plug-in.  Your plug-in properties file and plug-in code may not match appropriately. Look at the Tomcat log for errors.
menu.	The log file is localhost.date.log. This log file is in SymantecDLP\Protect\logs\tomcat.
	To verify that your plug-in is loaded, look for Enforce system event (2122). This event lists all the plug-ins that are loaded.

### Troubleshooting suggestions (continued) **Table 58-4**

Issue	Suggestions
Your plug-in does not execute successfully.	Check the incident snapshot history for messages from your plug-in and the plug-in framework.
	For Smart Responses, look at the Tomcat log for errors. This log is in  SymantecDLP\Protect\logs\tomcat. The log file is localhost. date.log.  For automated responses, look at the VontuIncidentPersister.log debug log file.

# Setting up scans of file shares

This chapter includes the following topics:

- Setting up server scans of file systems
- Supported file system targets
- Automatically discovering servers and shares before configuring a file system target
- Automatically discovering open file shares
- About automatically tracking incident remediation status
- Excluding internal DFS folders
- Configuring scans of Microsoft Outlook Personal Folders (.pst files)
- Configuring and running scans of file systems
- Optimizing file system target scanning
- Configuring Network Protect for file shares

# Setting up server scans of file systems

Network Discover scans network file servers and shared resources ("shares") such as disk drives or directories to discover confidential data. Network Discover supports CIFS-compliant file servers, and file shares using CIFS, NFS, DFS, or any other client. Network Discover can also scan Microsoft Outlook Personal Folders (.pst files) on network file shares.

To set up scanning of file systems, complete the following process:

Step	Action	Description
1	Verify that your network file system is on the list of supported targets.	See "Supported file system targets" on page 1242.
2	Optional: Run a Content Root Enumeration scan to automatically discover file system content roots within your domain.	See "Automatically discovering servers and shares before configuring a file system target" on page 1243.
3	Go to <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create a new target for a file system and to configure scanning of file systems.	See "Configuring and running scans of file systems" on page 1254.
4	Set any additional scan target configuration options.  For scanning of Microsoft Outlook Personal Folders, verify that the option is set.	See "Network Discover scan target configuration options" on page 1191.  See "Configuring scans of Microsoft Outlook Personal Folders (.pst files)" on page 1253.
5	To automatically move or quarantine files, configure Network Protect.	See "Configuring Network Protect for file shares" on page 1258.
6	Start the file system scan.  Go to Manage > Discover Scanning > Discover Targets.	Select the scan target from the target list, then click the Start icon.
7	Verify that the scan is running successfully.	See "About the Network Discover scan target list" on page 1210.

Table 59-1 Setting up a network file system scan

# **Supported file system targets**

The File System target supports scanning of the following network file systems.

Supported file servers:

CIFS Servers only

Supported file shares:

- CIFS on Windows Server 2008 and 2012
- NFS on Red Hat Enterprise Linux 5.x and 6.x
- DFS scanning on Windows 2008 and 2012.

**Note:** DFS is not supported with Network Protect.

In addition, the File System target supports scanning of the following file types:

- Microsoft Outlook Personal Folders (.pst files) created with Outlook 2007, 2010, and 2013.
  - The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2007 or later must be installed on that system. See "Configuring scans of Microsoft Outlook Personal Folders (.pst files)" on page 1253.
- File systems on UNIX systems, even if they are not exposed as CIFS or NFS shares.

Use the SFTP protocol to provide a method similar to the scans of file shares. You can also scan the local file system on a Linux Network Discover Server by listing the path name in the content root. For example, you can enter /home/myfiles.

# Automatically discovering servers and shares before configuring a file system target

Auto-discovery of servers and shares (Content Root Enumeration) enables you to locate servers and shares within a domain and filter them by IP range or server name. Share discovery works only for CIFS-compliant file servers, including those with DFS file shares. Content Root Enumeration scans produce a list of servers and shares that you can use directly in file system targets for Discover scanning. or export to a CSV file. A Content Root Enumeration scan does not scan the content of the servers and shares it discovers, but it enables you to find servers and shares in your domain and configure automated scanning of them.

Content Root Enumeration scans require an LDAP directory server connection. Also, the Enforce Server must have access to all servers and shares you wish to scan.

See "Configuring directory server connections" on page 127.

See "Configuring and running scans of file systems" on page 1254.

# Working with Content Root Enumeration scans

Follow these procedures to create, start, and stop Content Root Enumeration scans, and to view discovered content roots.

### To create a Content Root Enumeration scan

- Configure your LDAP directory server connection. Ensure that your directory credentials have read and list privileges for all computer objects you wish to scan.
  - See "Configuring directory server connections" on page 127.
- 2 In the Enforce Server administration console, go to Manage > Discover Scanning > Content Root Enumeration.
- 3 Click Add Scan. The Content Root Enumeration Scan Configuration page appears.
- 4 In the **General** section, enter a name for your scan in the **Name** field.
- 5 Select a directory connection.
- Specify your **Enumerate shares** preference:
  - To list servers and file shares, click Yes.
  - To list only servers, click No, only enumerate servers.
- 7 In the **Filters** section, select at least one filter for your scan:
  - IP Range: Specify an IP range to scan for content roots.
  - Server Names: Specify one or more server name filters. Use the drop-down menu to refine your filter.
- 8 Click Save.

### To start or stop a Content Root Enumeration scan

- 1 In the Enforce Server administration console, go to Manage > Discover Scanning > Content Root Enumeration.
- 2 Select the scan or scans you want to start or stop.
- 3 Do one of the following:
  - To start a scan, click **Start**.
  - To stop a running scan, click **Stop**.

### To view discovered content roots

- In the Enforce Server administration console, go to **Manage > Discover** Scanning > Content Root Enumeration.
- Click the link in the Content Roots column of your desired scan to see a list of content roots.
- 3 To export the list of content roots in .csv format, click **Export to CSV** in the Content Roots dialog box.

You can use the exported .csv file to populate a Discover File System target. See "Configuring and running scans of file systems" on page 1254.

### **Configuration options for Content Root Enumeration scans**

You can find configuration options for Content Root Enumeration scans in the Manager.properties file in the configuration directory:

\SymantecDLP\Protect\config on Microsoft Windows platforms, /opt/SymantecDLP/Protect/config on Linux platforms. These default settings should perform well in most cases.

**Table 59-2** 

Configuration property	Default value	Description
content_root_enumeration.scanResultThreshold	10000	The maximum number of content roots to be discovered in a Content Root Enumeration scan. If the number of content roots in the scan exceeds the result threshold, Symantec Data Loss Prevention displays an error. This threshold prevents your Content Root Enumeration scans from returning an excessive number of content roots for use in a Discover File System target.

(continued) **Table 59-2** 

Configuration property	Default value	Description
content_root_enumeration.maximumParallelScanCount	5	The maximum number of Content Root Enumeration scans that Symantec Data Loss Prevention can run in parallel. If the maximum parallel scan count is reached, additional scans are queued.
content_root_enumeration.scan_log.location	<pre>Windows: \SymantecDLP\Protect\logs Linux: /opt/SymantecDLP/Protect/logs</pre>	The location of the Content Root Enumeration scan detail log files.
content_root_enumeration.scan_log.limit	5000000	The maximum size, in bytes, of each scan detail log file.
content_root_enumeration.scan_log.count	15	The maximum number of scan detail log files in use at any given time.
content_root_enumeration.scan_log.append	true	The Boolean value that specifies whether or not Symantec Data Loss Prevention appends log results to the end of each scan detail log file.
content_root_enumeration.scan_log.encoding	UTF-8	The character set Symantec Data Loss Prevention uses when writing to the scan detail log file.

# Troubleshooting Content Root Enumeration scans

You can view both scan warnings and log files for Content Root Enumeration scans. These warnings and logs can be useful for troubleshooting your Content Root Enumeration scans.

Content Root Enumeration scan warnings are non-terminal errors, such as connection timeouts or DNS issues, that occur during the scan. If such errors occur during a Content Root Enumeration scan, a link appears in the Alerts column on the Manage > Discover Scanning > Content Root Enumeration page for that scan. You can view these warnings by following this procedure:

### To view Content Root Enumeration scan warnings

- In the Enforce Server administration console, go to Manage > Discover Scanning > Content Root Enumeration.
- 2 Click the link in the Alerts column for the scan warnings you want to view. The Scan Warnings dialog box appears.
- To export the list of scan warnings to a .csv file, click Export to CSV in the Scan Warnings dialog box.

Log files are available in the logs directory: \SymantecDLP\Protect\logs on Microsoft Windows platforms, /opt/SymantecDLP/Protect/logs on Linux platforms. Content Root Enumeration logs are named using this format: ContentRootEnumerationScanDetail-scan name0.log. Content Root Enumeration log files list every discovered content root, as well as all warnings and errors occurring during the scan.

# Automatically discovering open file shares

Symantec Data Loss Prevention can automatically discover open shares on a specified CIFS server. You specify the UNC path or SMB URL and Symantec Data Loss Prevention automatically finds and scans open file shares on that server.

See "To set up a new file system target" on page 1254.

You can automatically discover administrative shares corresponding to logical drives such as C\$ or D\$.

### To discover administrative shares automatically

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Create or select a File System Server target.
- 3 On the Advanced tab of the Edit File System Target page, select Scan Administrative Shares.

# About automatically tracking incident remediation status

You can configure Network Discover to automatically track the remediation status of file system target incidents.

During the first Network Discover scan for a given file system target, incident metadata (resource name, policies violated, and so on) is added to a new Discover incident remediation tracking catalog. If during a subsequent scan an incident stored in the catalog does not appear in the scan results, Network Discover marks the incident as remediated with one of the following status indicators:

- Item modified. The item has been modified and no longer violates a policy. In the case where both the item and policy have changed, the incident will be remediated as **Item modified**. This option is off by default.
- Policy modified. The policy that the incident violated has changed. In the case where both the item and policy have changed, the incident will be remediated as Item modified. This option is off by default.
- Item no longer exists. The item has been moved, deleted, or renamed. This option is on by default.

To prevent incidents from being automatically remediated in error, Network Discover will not mark an incident as remediated if it is excluded from a scan due to:

- Incremental scanning
- Date filtering
- Size filtering
- Include or Exclude filters

The incident remediation catalog is contained in an Apache Derby database running under the BoxMonitor process. The master catalog is stored on the Enforce Server, and each detection server has its own local version of the catalogs. The catalogs are synchronized to ensure that the Enforce Server and all Network Discover detection servers track incident remediation status correctly.

You can set your incident remediation tracking preferences on the Advanced tab of your file system target.

See "Configuring and running scans of file systems" on page 1254.

You can configure options for automated incident remediation tracking, such as the location of the catalog files, expiration period of temporary files, and so on.

See "Configuration options for Automated Incident Remediation Tracking" on page 1249.

You can view the latest remediation status of an incident in the incident snapshot.

See "Discover incident snapshots" on page 991.

You can also filter and summarize Network Discover reports by incident remediation status.

See "About filters and summary options for reports" on page 1046.

# Troubleshooting automated incident remediation tracking

Automated incident remediation tracking does not work if you have enabled incident thresholding. If you have enabled automated incident remediation tracking for a file system target but do not see any tracking information, ensure that you have disabled incident thresholding.

See "Creating an inventory of the locations of unprotected sensitive data" on page 1206.

You can view a log file for the incident remediation catalog on the detection server at this location:

SymantecDLP/Protect/logs/debug/DetectionServerDatabase%g.log, Where %g is an integer starting at 0. Logs for incidents tracked with this feature are sent to the FileReader%.log and IncidentPersister%.log.

### You can set the incident remediation catalog log level in the

SymantecDLP/Protect/config/DetectionServerDatabaseLogging.properties file:

**Table 59-3** Remediation tracking database logging options

Log Level	Description	
FINE	The Detection Server database heartbeats are logged at the FINE level.	
INFO	Database start and stop messages are logged at the INFO level.	
SEVERE	All unexpected database behavior throws an exception and appears in the log at the SEVERE level.	

# Configuration options for Automated Incident Remediation Tracking

You can set the following configuration options for Automated Incident Remediation Tracking in the SymantecDLP/Protect/config/protect.properties file. If you

have a multi-tier installation, there will be separate files for the Enforce Server and Network Discover Server.

Table 50 /

Table 59-4		
Property	Default value	Description
com.vontu.discover.detectionserver. remediation.detection. comm.maxfiles	15000	The maximum number of files stored in the Network Discover Server remediation tracking catalog directory before synchronization with the master catalog on the Enforce Server. If the number of catalog files exceeds this limit, Network Discover creates no new catalog entries until at least one file is synchronized.
<pre>com.vontu.discover.enforce. remediation.detection. comm.maxfiles</pre>	15000	The maximum number of files stored in the Enforce Server remediation tracking master catalog directory before synchronization with the local catalog on the Network Discover Server. If the number of catalog files exceeds this limit, Network Discover creates no new master catalog entries until at least one file is synchronized.

**Table 59-4** (continued)

Property	Default value	Description
com.vontu.discover.detectionserver. remediation.detection. catalogfolder.checkperiod	10000	The frequency, in milliseconds, with which the Network Discover Server checks the remediation tracking catalog directory for the number of catalog files queued for synchronization with the master catalog on the Enforce Server.
com.vontu.discover.enforce. remediation.detection. catalogfolder.checkperiod	10000	The frequency, in milliseconds, with which the Enforce Server checks the remediation tracking master catalog directory for the number of catalog files queued for synchronization with the catalog on the Network Discover Server.
com.vontu.discover.detectionserver. remediation.detection. catalog.tempfile.expirationhours	24	The expiration period, in hours, of temporary files in the remediation tracking catalog directory.
com.vontu.discover.enforce. remediation.detection. catalog.tempfile.expirationhours	24	The expiration period, in hours, of temporary files in the remediation tracking master catalog directory.

(continued) **Table 59-4** 

Property	Default value	Description
com.vontu.discover.detectionserver. remediation.detection. catalog.folder	C:/SymantecDLP/Protect/ scan/catalog	The directory containing the Network Discover Server remediation tracking catalog files.
com.vontu.discover.enforce. remediation.detection. catalog.folder	C:/SymantecDLP/Protect/ scan/catalog	The directory containing the Enforce Server remediation tracking master catalog files.
com.vontu.discover.detectionserver. remediation.detection. threadpoolsize	5	The size of the threadpool used for automated incident remediation tracking on the Network Discover Server.
com.vontu.discover.enforce. remediation.detection. threadpoolsize	5	The size of the threadpool used for automated incident remediation tracking on the Enforce Server.
com.vontu.detectionserver.database.home	C:/SymantecDLP/Protect/ scan/catalog	The directory containing the Network Discover Server remediation tracking database.
com.vontu.detectionserver.database.port	1527	The port used by the Network Discover Server remediation tracking database.
com.vontu.manager.incidents.dir	./incidents	The directory containing offline incidents on the Enforce Server.

# **Excluding internal DFS folders**

By default, DFS file share scans include the dynamic internal DFS folders. Because these folders do not contain your organization's confidential information you can safely exclude them from your scans.

### To exclude DFS internal folders

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click the name of the scan where you want to add the exclude filter for the DFS internal folders.
- Click the **Scanned Content** tab.
- In the Exclude Filters field, type /DfsrPrivate/\*.
- Click Save.

# Configuring scans of Microsoft Outlook Personal Folders (.pst files)

You can scan Microsoft Outlook Personal Folders (.pst files) on file shares. The scan supports Microsoft Outlook Personal Folders (.pst files) that were created with Outlook 1997-2002, 2003, 2007, and 2010.

See "Configuring and running scans of file systems" on page 1254.

The following notes pertain to scanning .pst files:

- The Network Discover Server scanning this target must be running a 64-bit Windows operating system, and Outlook 2010 or 2013 64-bit clients must be installed on that system.
- Outlook must be the default email client on the Network Discover Server scanning this target.
- Network Protect is not supported for .pst files, even if the files are on CIFS shares.
- After the initial base scan, incremental scanning scans the entire .pst file if the last modified date changes.
- The date filter and size filter apply to the entire .pst file, not to individual emails or other items within the file.
- The .pst files cannot be scanned in parallel. If the scans that run in parallel start scanning .pst files, then the scans are serialized.

### To configure scanning of Microsoft Outlook Personal Folders

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Set up scanning of the file share containing the Microsoft Outlook Personal Folders.
  - See "Configuring and running scans of file systems" on page 1254.
- 3 On the Advanced tab, check the box Scan PST files. (The box is checked by default.)

# Configuring and running scans of file systems

Before you run a scan, you must set up a target using the following procedure.

### To set up a new file system target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click **New Target**, and use the pull-down menu to select the specific target type.
- 3 On the **General** tab, type the **Name** of this Discover target.
  - Type a unique name for the target, up to 255 characters.
- Select the **Policy Group**.
  - If no other policy group has been selected, the Default Policy group is used. To apply a policy group, select the policy group to use for this target. You can assign multiple policy groups to a target.
  - You can define policy groups on the Policy Group List page.
- 5 Select the Discover Server (or multiple Discover Servers) where you want to run the scan.
  - If you select more than one server, Symantec Data Loss Prevention automatically selects one of the servers when the scan starts.
  - Only the detection servers that were configured as Discover Servers appear on the list. If there is only one Discover Server on your network, the name of that server is automatically specified. You should configure your Discover Servers before you configure targets. You must specify at least one server before you can run a scan for this target.
- Under Scan Type, select Scan only new or modified items (incremental scan). This option is the default for new targets.

- If you have changed the policy or other definitions in an existing scan, you can set up the next scan as a full scan. Select the following option: Scan all items for the next scan. Subsequent scans will be incremental.
- If you always want to scan all items in this target, select the following option: Always scan all items (full scan)
- Specify scheduling options. 7

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the schedule drop-down list to display additional fields. Choose Pause Scan between these times to automatically pause scans during the specified time interval. You can override the pause window of a scan target by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon for the target entry.

8 On the **Scanned Content** tab, select or type the credentials.

The credentials you provide must have both Read permission and Write Attributes permission on the scan target. Write Attributes permission is required to update the "last accessed" date.

You can specify a default user name to use for access to all file systems.

The password must not contain the quotation mark character. If any of your passwords contain a quotation mark character, those file systems are not mounted for scanning.

If you need to use quotation mark characters in passwords, you can use JCIFS. The default mount process uses the CIFS client. If the default mount does not work, the mount task can use the Java-based CIFS client by setting filesystemcrawler.use.jcifs=true in the properties file Crawler.properties.

9 Under Content Roots, enter the item to be scanned.

Select one of the following methods of entering file systems:

Scan Content Roots from an uploaded file

Create and save a plain text file (.txt or .csv) listing the servers you want to scan. Then click Browse to locate the list and Upload File to import it. Create a file using an ASCII text editor and type one file server or share per line. Do not include a user name and password. By default, Symantec Data Loss Prevention interprets these as Server Message Block (SMB) paths. If you want to specify NFS paths, include nfs in the paths.

```
\\server\marketing
nfs:\\share\marketing
//server/engineering/documentation
/home/protect/mnt/server/share/marketing
c:\share\engineering
```

### Specify content roots

 Select Add Content Roots > By Direct Entry to use a line editor to specify the servers or shares you want to scan. Information that is entered here takes precedence over the default values and applies only to the path specified.

```
\\server\share
\\server.company.com
smb://server.company.com
\\10.66.23.34
```

Select Add Content Roots > From a Content Root Enumeration scan to import content roots from a Content Root Enumeration scan. Select the scan to import in the **Import Content Root Enumeration** scan results dialog box.

If your content root list includes a large number of content roots, you can filter the list to include only those content roots that are relevant to your Discover Target scan. In the **Content Roots** section, click **Filters**, then enter your filter text. For example, to see only shares on a server named my company, enter \my company in the Filters text field.

To delete content roots from your target, select the content roots from the list and click **Delete**.

- 10 On the Filters tab, specify include and exclude filters, size filters, and date filters.
  - Use **Include Filters** and **Exclude Filters** to specify the files that Symantec Data Loss Prevention should process or skip. Note that you must specify absolute paths. If the field is empty, Symantec Data Loss Prevention performs matching on all files in the file share. If you enter any values for the Include Filters, Symantec Data Loss Prevention scans only those files or documents that match your filter. Delimit entries with a comma, but do not use any spaces. When both **Include Filters** and **Exclude Filters** are present, Exclude Filters take precedence.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

When scanning DFS shares, exclude the internal DFS folder.

See "Excluding internal DFS folders" on page 1253.

When scanning shares on a NetApp filer with the Snapshot application, exclude the .snapshot folder. This folder is usually at the base of the file system or network share; for example, \myshare\.snapshot.

- Specify size filters.
  - The size filters let you exclude files from the matching process based on their size. Symantec Data Loss Prevention includes only the files that match your specified size filters. If you leave these fields empty, Symantec Data Loss Prevention performs matching on files or documents of all sizes.
- Specify date filters. The date filters let you include files from the matching process based on their dates. Any files that match the specified date filters are scanned.
- 11 On the **Advanced** tab, specify your Remediation Detection preferences to automatically detect incident remediation status:
  - Item Modified: Automatically detect if an incident has been remediated by modifying the offending file.
  - Policy Modified: Automatically detect if an incident has been remediated by a change in your policy.
  - Item No Longer Exists: Automatically detect if an incident has been remediated by deletion or removal.

See "About automatically tracking incident remediation status" on page 1248.

12 On the **Advanced** tab, select options to optimize scanning.

See "Optimizing file system target scanning" on page 1257.

# Optimizing file system target scanning

To optimize scans of your File System scan target, you can configure throttling options, set an incident threshold for scanning (Inventory Scanning), omit or select Outlook .pst files, and enable or disable scans of administrative shares.

### To throttle a file system target scan

- Go to the **Advanced** tab of your target definition.
- 2 In the File Throttling field, type the maximum number of files to be processed per minute.
- In the Byte Throttling field, type the maximum amount of data to be processed per minute. Select bytes, kilobytes (KB), or megabytes (MB) from the drop-down list.

### To set an incident threshold

- 1 Go to the **Advanced** tab of your target definition.
- 2 In the **Incident Threshold** field type the maximum number of incidents to be created from a single file share (Content Root) or server (Machine).
- 3 Select Count Incidents By: Content Root or Machine.

A Content Root is one file share on the list from the Scanned Content tab. When the incident threshold is reached, the scan moves to the next file share.

A **Machine** is a physical computer. When the incident threshold is reached, the scan moves to the next item on the list to scan. If that item is on the same physical computer as the previous item, it is skipped. The physical computer name must be exactly identical in the list of items to scan for Network Discover to recognize that it is the same computer. For example, \\localhost\myfiles and \\127.0.0.1\myfiles are treated as different computers, even though they are logically the same.

If you use autodiscovery to scan open shares on a specified file server, the content root and machine are the same thing.

### To scan administrative shares

- Go to the **Advanced** tab of your target definition.
- In the Administrative Shares Scanning section, select Scan Administrative Shares.

You can also set up scanning of Outlook .pst files.

See "Configuring scans of Microsoft Outlook Personal Folders (.pst files)" on page 1253.

# **Configuring Network Protect for file shares**

Use Network Protect to automatically copy or quarantine to a secure location the confidential files that are found on public shares.

Network Protect is only available for server-based scanning of CIFS shares. Network Protect is not supported for .pst files.

With Network Protect enabled, a tab appears on the Add File System Target page that contains the Network Protect remediation options. To use Network Protect, you must have both a policy and a response rule configured in the Enforce Server administration console. Also, the scan credentials (user name and password) must be present on the **Scanned Content** tab for this target.

The following procedure provides an overview of the process.

### To set up Network Protect for file shares

Create a policy with a response rule. Go to Manage > Policies > Response Rules and click Add Response Rule.

See "About response rules" on page 875.

- 2 Select Automated Response.
- 3 Click Next.
- For the Action, select either Network Protect: Copy File or Network Protect: Quarantine File.

For the Quarantine File action, you can optionally leave a marker file in place of the file that was removed by checking the Marker File check box. Type the marker text in the Marker Text box. The marker file is a text file. The marker text can contain substitution variables. Click inside the Marker Text box to see a list of insertion variables.

If the original file was of some other file type, the original file is moved to the quarantine area. The marker file has the original file name plus a .txt extension. The default file extensions that are retained are listed in the properties file ProtectRemediation.properties. The retained file extensions include txt, doc, xls, ppt, java, c, cpp, h, and js. For example, a file that is named myfile.pdf would have a marker file name of myfile.pdf.txt.

You can create a new subdirectory for the guarantined files from each scan (the default). You can change the default and append the scan information to the file name (versioning) in one quarantine directory. Edit the properties file ProtectRemediation.properties to change the default.

- 5 Click Save.
- 6 Add a new policy, or edit an existing policy.

See "Configuring policies" on page 326.

- 7 Click the **Response** tab.
- In the pull-down menu, select one of the response rules that you previously 8 created.
- 9 Click Add Response Rule.

This response rule then specifies the automated response when this policy triggers an incident during the scanning of a file.

Several response rules with different conditions can exist for a policy.

10 Create a new file system Network Discover target, or edit an existing target.

See "Configuring and running scans of file systems" on page 1254.

11 With Network Protect enabled in the license, a **Protect** tab appears on the **File System** target page that contains the Network Protect remediation options.

Under Allowed Protect Remediation, choose whether the file should be copied or guarantined (moved) to protect the information.

This selection must match the **Action** selection from the response rule.

Also, a response rule with that action (copy or quarantine) should exist within one of the policies that are selected for this file system target.

12 Under Copy/Quarantine Share, specify the share where files are quarantined or copied.

Optionally, you can select a named credential from the credential store in the Use Saved Credentials drop-down menu.

13 Under Protect Credential, specify the write-access credential for the location of the file that was scanned.

To move the files for quarantine during remediation, the Network Discover target definition must have write access for both the guarantine location and the original file location. Specify the path (location) where the files are copied or guarantined. Type the write-access user name and password for that location.

Normally, scanned shares require only read-access credentials (for example, if the Copy option was selected).

Specify the share write-access credential, if it is different from the read-access credential.

Optionally, you can select a named credential from the credential store in the Use Saved Credentials drop-down menu.

## Setting up scans of Lotus Notes databases

This chapter includes the following topics:

- Setting up server scans of Lotus Notes databases
- Supported Lotus Notes targets
- Configuring and running Lotus Notes scans
- Configuring Lotus Notes DIIOP mode configuration scan options

### Setting up server scans of Lotus Notes databases

You can configure scans of Lotus Notes repositories. Symantec Data Loss Prevention supports DIIOP mode scanning only.

See "Configuring and running Lotus Notes scans" on page 1262.

To set up scanning of Lotus Notes databases, complete the following process:

**Table 60-1** Setting up a Lotus Notes database scan

Step	Action	Description
1	Verify that your Lotus Notes database is on the list of supported targets.	See "Supported Lotus Notes targets" on page 1262.
2	Configure the scan for Lotus Notes DIIOP mode.	See "Configuring Lotus Notes DIIOP mode configuration scan options" on page 1265.
3	Click Manage > Discover Scanning > Discover Targets to create a Lotus Notes target and to configure scans of Lotus Notes databases.	See "Configuring and running Lotus Notes scans" on page 1262.

Step	Action	Description
4	Set any additional scan options for the Lotus Notes target.	See "Network Discover scan target configuration options" on page 1191.
5	Start the Lotus Notes database scan.  Click Manage > Discover Scanning > Discover Targets.	Select the scan target from the list, then click the Start icon.
6	Verify that the scan is running successfully.	See "Managing Network Discover target scans" on page 1209.

Table 60-1 Setting up a Lotus Notes database scan (continued)

### Supported Lotus Notes targets

The Lotus Notes target supports scanning of the following versions:

- Lotus Notes 7.0
- Lotus Notes 8.0
- Lotus Notes 8.5.x

The files Notes.jar and NCSO.jar are in the Lotus Notes client installation directory. The manifest version number of these files depend on the Domino server version.

- Version 7 has a manifest version in the JAR file of 1.4.2
- Version 8 has a manifest version in the JAR file of 1.5.0

### Configuring and running Lotus Notes scans

Before you run a scan, you must set up a target.

#### To set up a new target for the scan of Lotus Notes databases

Specify the content root for a Lotus Notes scan as either one Domino server, or a list of Domino servers.

Specify the databases to scan as follows:

Individual

Click Add to specify the servers you want to scan. Server credential information that is entered here takes precedence over the default values and applies only to the server specified.

[hostname, username, password]

For a native mode configuration, you can use the name "local" in the list of Domino servers. Specifying "local" includes the local databases visible to the client only to be scanned. For example, instead of the URI enter the following text:

local

#### Upload Servers List

Create and save a plain text file (.txt) with the servers you want to scan. The server credential cannot be specified in this text file. The user name and password from the **Scanned Content** tab of the **Add Lotus Notes** Target page are used .

Example of the first few Domino servers in the list:

```
dominoserver1.company.com
dominoserver2.company.com
dominoserver3.company.com
```

2 On the **Filters** tab, select path filters.

Use the Include Filters and Exclude Filters fields to specify the Lotus Notes database names that Symantec Data Loss Prevention should target. The filters match the full path of the database URI. If the field is empty, Symantec Data Loss Prevention scans all databases in all specified Domino Servers. Delimit entries with commas. If a database URI matches both an include and an exclude filter, the exclude filter takes precedence, and the database is not scanned.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

3 On the **Filters** tab, select date filters.

> Specify the date filters to exclude Lotus Notes documents from the scan based on their dates. Only the documents that match the specified date filters are included.

4 On the **Filters** tab, select a Differential scan (optional).

Select Only Scan files added or modified since the last full scan to have Symantec Data Loss Prevention scan only the items or the documents that have been added or modified since the last full scan. The first scan has to be a full (initial base) scan. A full scan occurs if you select this option before Symantec Data Loss Prevention scans this target for the first time.

5 On the **Filters** tab, select a Differential scan (optional).

Select Only Scan files added or modified since the last full scan to have Symantec Data Loss Prevention scan the documents that have been added or modified since the last scan. If you select this option before Symantec Data Loss Prevention scans this target for the first time, the first scan runs as a full scan.

6 On the **General** tab, select scheduling options.

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the Schedule drop-down list to display additional fields. Choose Pause Scan between these times to automatically pause scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon for the target entry.

7 Select Size Filters.

> Specify the size filters to exclude documents from the target based on their size. Symantec Data Loss Prevention includes only the documents that match your specified size filters. If you leave this field empty, Symantec Data Loss Prevention includes all documents.

8 Enter Credentials (default and overriding).

You can specify a default user name and password to access all Domino servers that are specified in the target. Credentials can be overridden for a server by editing a single entry in the list of Domino servers. Credentials for a single entry are possible only if the list is created with individually entered server names. Credentials for a single entry are not possible in an uploaded text file that contains the list of servers.

- Select the Advanced tab for options to optimize scanning. On the **Advanced** tab, you can configure throttling options or Inventory Mode for scanning.
  - Throttling Options Enter the maximum number of documents to be processed per minute or the maximum number of bytes to be processed per minute. For bytes, specify the unit of measurement from the drop-down list. The options are bytes, KB (kilobytes), or MB (megabytes).
  - Inventory Scanning Enter the number of incidents to produce before moving on to the next Domino server that is specified in the Scanned Content tab. To audit whether confidential data exists on a target, without scanning all of it, set up Inventory Mode for scanning. Setting incident thresholds can improve

the performance of scanning by skipping to the next server to scan, rather than scanning everything.

See "Creating an inventory of the locations of unprotected sensitive data" on page 1206.

### Configuring Lotus Notes DIIOP mode configuration scan options

In the file Crawler.properties, when lotusnotescrawler.use.diiop is set to true, DIIOP (CORBA) is used to scan a Domino server. The scanner connects directly to the Domino server with HTTP and DIIOP.

#### To configure a Lotus Notes DIIOP mode configuration for scanning

Copy the Lotus Notes Java library files Notes. jar and NCSO. jar to the SymantecDLP/Protect/plugins directory.

They can be found in the installation directories of a Lotus Notes client, and a Lotus Domino server with the Domino Designer installed.

The Notes.jar file is in the following Lotus Notes client default installation directories:

Lotus Notes 8

C:\Program Files\IBM\lotus\notes\jvm\lib\ext\Notes.jar

Lotus Notes 7

C:\Program Files\lotus\notes\jvm\lib\ext\Notes.jar

Lotus Notes 6.5

C:\Program Files\lotus\notes\Notes.jar

Use the version of the JAR file corresponding to the version of the Lotus Notes client.

See "Supported Lotus Notes targets" on page 1262.

The NCSO. jar file is in the following Lotus Domino server default installation directories, when the Domino Designer is installed:

Lotus Notes 8

C:\Program Files\IBM\lotus\Notes\Data\domino\java\NCSO.jar

#### Lotus Notes 7

C:\Program Files\lotus\notes\data\domino\java\NCSO.jar

#### Lotus Notes 6.5

C:\Program Files\lotus\notes\data\domino\java\NCSO.jar

2 In the file Crawler.properties, set the following property:

```
lotusnotescrawler.use.diiop = true
```

- 3 Start the HTTP service on the Domino server.
- 4 Start the DIIOP service on the Domino server.
- 5 On the Domino server, set the Allow HTTP connections to browse databases setting to true.
- When creating targets, enter the credentials of a user who has an Internet password.

# Setting up scans of SQL databases

This chapter includes the following topics:

- Setting up server scans of SQL databases
- Supported SQL database targets
- Configuring and running SQL database scans
- Installing the JDBC driver for SQL database targets
- SQL database scan configuration properties

### Setting up server scans of SQL databases

You can configure scanning of Oracle, SQL Server, or DB2 databases.

See "Configuring and running SQL database scans" on page 1268.

To set up scanning of SQL databases, complete the following process:

**Table 61-1** Setting up an SQL database scan

Step	Action	Description
1	Verify that your SQL database is on the list of supported targets.	See "Supported SQL database targets" on page 1268.
2	Click Manage > Discover Scanning > Discover Targets to create an SQL database target and to configure scans of SQL databases.	See "Configuring and running SQL database scans" on page 1268.

Step	Action	Description
3	Set any additional scan options for the SQL database target.	See "Network Discover scan target configuration options" on page 1191.
4	Install the JDBC driver for the SQL database, if needed.	See "Installing the JDBC driver for SQL database targets" on page 1271.
5	Start the SQL database scan.  Click Manage > Discover Scanning > Discover Targets.	Select the scan target from the target list, then click the Start icon.
6	Verify that the scan is running successfully.	See "Managing Network Discover target scans" on page 1209.

Table 61-1 Setting up an SQL database scan (continued)

### Supported SQL database targets

The following SQL Databases were tested with Network Discover Target scans:

- Oracle 10g (the vendor\_name is oracle)
- SQL Server 2005 (the *vendor name* is sqlserver)
- DB2 9 (the vendor\_name is db2)

Contact Symantec Data Loss Prevention support for information about scanning any other SQL databases.

### Configuring and running SQL database scans

You can configure and run scans on SQL databases to identify which databases contain confidential data, or to locate the inappropriate presence of confidential data.

Scanning of SQL databases occurs for a specific set of column data types. The SQL Database scan extracts data of the following Java Database Connectivity (JDBC) types: CLOB, BLOB, BIGINT, CHAR, LONGVARCHAR, VARCHAR, TINYINT, SMALLINT, INTEGER, REAL, DOUBLE, FLOAT, DECIMAL, NUMERIC, DATE, TIME, and TIMESTAMP. The mapping between these column types and those of a specific database depends on the implementation of the JDBC driver for the scan.

#### To set up a scan for an SQL Database

- Select one of the following methods for entering the databases:
  - Upload a file with the list of databases Create and save a plain text file (.txt) with the servers you want to scan. Click Browse to locate the list and Upload to import it. The user name and password that is specified on the Scanned Content tab of the Add SQL Database Target page is used.

Enter the databases using the following syntax. The vendor name can be oracle, db2, or sqlserver. The data source is the subname of the JDBC connection string for that driver and database. The documentation for the JDBC driver describes this subname. You can optionally enter the maximum rows to scan per table in the database.

```
vendor name:datasource[, maximum-rows-to-scan]
```

#### For example:

```
oracle:@//oracleserver.company.com:1521/mydatabase
db2://db2server.company.com:50000/mydatabase,300
```

For some SQL Servers, you must also specify the SQL instance name, as in the following example:

```
sqlserver://sqlserver.company.com:1433/mydatabase;
instance=mvinstance
```

 Manually enter the databases into the user interface Click the **Add** option to use a line editor to specify the databases you want to scan. SQL Database information that is entered here takes precedence over the default values and applies only to the database specified. You can optionally enter the maximum rows to scan per table in the database. Use the following syntax:

```
vendor-name:datasource[, [username, password]
[, maximum-rows-to-scan]]
```

2 On the **Filters** tab, enter the optional Include and Exclude filters.

Use the Include Filters and Exclude Filters to specify SQL databases and the tables that Symantec Data Loss Prevention should process or skip.

When both Include Filters and Exclude Filters are used, the Exclude Filters take precedence. Any table that matches the Include Filters is scanned, unless it also matches the Exclude Filters, in which case it is not scanned.

If the Include Filters field is empty, Symantec Data Loss Prevention performs matching on all tables. These tables are returned from the table query of the target SQL databases. If you enter any values in the field, Symantec Data Loss Prevention scans only those databases and tables that match your filter.

The syntax is a pattern for the database, a vertical bar, and a pattern for the table name. Multiple patterns can be separated with commas. Standard pattern matching applies. For example, "?" matches a single character.

Because the table name matching is not case-sensitive for many databases, upper case conversion occurs. The table name in the pattern and the table name it is matched against are converted to upper case before the match.

The following example would match the employee table in all databases.

```
*|employee
```

The following example would match all tables in all Oracle databases.

```
oracle:*/*
```

For SQL Server 2005 and DB2, the default table query returns table names in the format schema name.table name. Include Filters and Exclude Filters for SQL Server and DB2 should match this format.

See the following examples:

```
sqlserver: * | HRschema.employee
sqlserver: * | *.employee
```

On the **General** tab, select scheduling options.

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the Schedule drop-down list to display additional fields. Choose Pause Scan between these times to automatically pause scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon in the target entry.

- Select the **Advanced** tab for options to optimize scanning. On the **Advanced** tab, you can configure throttling options or Inventory Mode for scanning.
  - Throttling Options Enter the maximum number of rows to be processed per minute or the maximum number of bytes to be processed per minute. If you select both options, then the scan rate is slower than both options. The scan rate is slower than the specified number of rows per minute and the specified number of bytes per minute. For bytes, specify the unit of measurement from the drop-down list. The options are bytes, KB (kilobytes), or MB (megabytes).
  - Inventory Scanning Enter the number of incidents to produce before moving on to the next item to scan. The next item is the next database from the list in the Scanned **Content** tab. To audit whether confidential data exists on a target, without scanning all of it, set up Inventory Mode for scanning. Setting incident thresholds can improve the performance of scanning by skipping to the next item to scan, rather than scanning everything. See "Creating an inventory of the locations of unprotected sensitive data" on page 1206.

### Installing the JDBC driver for SQL database targets

A JDBC driver must be installed for each database type to be scanned.

#### To install the JDBC driver

- Obtain the relevant JDBC driver.
  - The Oracle driver is already installed with the Network Discover Server, in the default SQL drivers directory Protect/lib/jdbc. The JDBC driver is Oracle JDBC driver version 10.2.0.3.0.
  - For Microsoft SQL Server, the open source driver iTDS, can be obtained from Source Forge at http://jtds.sourceforge.net/.

The jTDS JDBC driver version 1.2.2 was tested with Network Discover.

- For DB2, the IBM driver JAR files are in the IBM DB2 distribution, under the java folder. They can be obtained from IBM at http://www.ibm.com/db2. The IBM JDBC driver version 1.4.2 was tested with Network Discover.
- 2 Copy the driver files to the default SQL drivers directory Protect/lib/jdbc.
- 3 Change the permissions of the JDBC driver files so that the Protect user has at least read permission.
- The sqldatabasecrawler.properties file may also need to be modified to specify the correct JAR names for the selected drivers.

See "SQL database scan configuration properties" on page 1272.

### SQL database scan configuration properties

The following configuration properties can be edited in the sqldatabasecrawler.properties configuration file on the Network Discover Server:

driver class.vendor\_name

Specifies the class name of the JDBC driver to use. The JAR file for this driver must be included in the directory that is named in sqldrivers.dir and must be named as driver jar. vendor name.

Example:

```
driver class.sqlserver = net.sourceforge.jtds.jdbc.Driver
```

 driver subprotocol.vendor name Specifies the subprotocol portion of the JDBC connection string. Example:

```
driver subprotocol.sqlserver = jtds:sqlserver
```

driver jar.vendor\_name

Specifies the list of JAR files that the driver requires. The JAR files are stored in the directory that is named in sqldrivers.dir.

See "Installing the JDBC driver for SQL database targets" on page 1271. Examples:

```
driver jar.sqlserver = jtds-1.2.2.jar
driver jar.db2 = db2jcc.jar, db2jcc license cu.jar
```

driver table query.vendor\_name

Specifies the query to execute to return a list of tables to scan. Typically, the query should return all user tables in the database. Note that the database account that issues this guery needs appropriate rights to be granted to it by the database administrator.

You must use an account to scan that can make the driver table query in sqldatabasecrawler.properties and return results. You can test the scan configuration by using sqlplus to log on as the scan user, and to run the query. If you get results, you have the permissions to complete the scan. If you do not get results, then you either have to change the query, or change the privileges for the scan user.

#### Example:

```
driver table query.sqlserver = SELECT table schema
+ '.' + table name FROM information schema.tables
```

#### driver row selector.vendor\_name

Specifies the format of the query to use to select the rows from the table. This vendor name varies, depending on the database. Examples are included in the sqldatabasecrawler.properties configuration file for the most common databases.

The following substitution variables are used in the query:

```
0=TABLENAME
1=COLUMNS
2=ROWNUM
```

#### Example:

```
driver row selector.sqlserver = SELECT TOP {2} {1} FROM {0}
```

#### quote\_table\_names.vendor\_name

Specifies whether table names are quoted before the row selection guery is created. Enabling this feature allows tables with numeric names to be scanned. For example, Payroll.1 becomes "Payroll"."1" when the name is quoted. Example:

```
quote table names.sqlserver=true
```

#### sqldrivers.dir

Specifies the location of the directory in which the JDBC driver JAR files are placed.

# Setting up scans of SharePoint servers

This chapter includes the following topics:

- Setting up server scans of SharePoint servers
- About scans of SharePoint servers
- Supported SharePoint server targets
- Access privileges for SharePoint scans
- About Alternate Access Mapping Collections
- Configuring and running SharePoint server scans
- Installing the SharePoint solution on the Web Front Ends in a farm
- Setting up SharePoint scans to use Kerberos authentication
- Troubleshooting SharePoint scans

### Setting up server scans of SharePoint servers

To set up scanning of SharePoint servers, complete the following process:

**Table 62-1** Setting up a SharePoint server scan

Step	Action	Description
1	Verify that your SharePoint server is on the list of supported targets.	See "Supported SharePoint server targets" on page 1277.

Table 6	Table 62-1   Setting up a SharePoint server scan (continued)		
Step	Action	Description	
2	Verify that you have sufficient permissions to install the SharePoint solution on the Web Front Ends in a Farm.  Also verify that the scan user has the permissions to run the scan of the SharePoint server.	See "Access privileges for SharePoint scans" on page 1277. See "Installing the SharePoint solution on the Web Front Ends in a farm" on page 1281.	
		See "Configuring and running SharePoint server scans" on page 1278.	
3	Install the SharePoint solution on the Web Front Ends in a Farm.	See "Installing the SharePoint solution on the Web Front Ends in a farm" on page 1281.	
4	Click Manage > Discover Scanning > Discover Targets to create a SharePoint target and to configure scans of SharePoint servers.	See "Configuring and running SharePoint server scans" on page 1278.	
5	Set any additional scan options for the SharePoint target.	See "Network Discover scan target configuration options" on page 1191.	
6	Start the SharePoint server scan.	Click Manage > Discover Scanning > Discover Targets.	
		Select the scan target from the target list, then click the Start icon.	
7	Verify that the scan is running successfully.	See "Managing Network Discover target scans"	

#### About scans of SharePoint servers

The Network Discover Server locates a wide range of exposed confidential data on SharePoint servers. It communicates with the Enforce Server to obtain information about policies and scan targets. It sends information about the exposed confidential data that it finds to the Enforce Server for reporting and remediation.

on page 1209.

The following types of SharePoint items are scanned:

- Wiki pages
- Blogs

- Calendar entries
- Tasks
- Project tasks
- Discussion entries
- Contact lists
- Announcements
- Links
- Surveys
- Issue tracking
- Custom lists
- Documents in the document library

Note: Only the latest version of a document is scanned.

The communication between the Discover Server and the SharePoint Web Front End (WFE) is SOAP-based.

Communication is secure when the SharePoint Web sites are configured to use SSL.

For HTTPS, validation of the server SSL certificate is not the default. To enable validation of the server SSL certificate, turn on the advanced setting Discover.ValidateSSLCertificates. Then import the server SSL certificate to the Discover Server.

See "Advanced server settings" on page 203.

See "Importing SSL certificates to Enforce or Discover servers" on page 197.

If the specified SharePoint site is configured to be on a port that is not the default (80), ensure that the SharePoint server allows the Discover Server to communicate on the required port.

The SharePoint solution uses Windows SharePoint Services (WSS) application programming interfaces. User access to the content is based on the rights for the specified user in SharePoint. Enter the user credentials to specify this user when you configure a SharePoint scan.

See "Configuring and running SharePoint server scans" on page 1278.

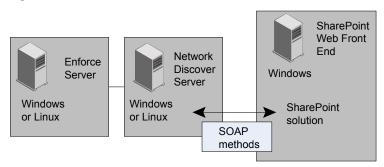


Figure 62-1 SharePoint communication with the Discover Server

### Supported SharePoint server targets

The following SharePoint server targets are supported:

- Microsoft Office SharePoint Server 2007, on Windows Server 2003, 32-bit or 64-bit, or Windows Server 2008 R1, 32-bit or 64-bit
- Microsoft Office SharePoint Server 2010, on Windows Server 2008 R2, 64-bit
- Microsoft Office SharePoint Server 2013, on Windows Server 2008 R2, 64-bit
- Microsoft Office SharePoint Online 2010
- Microsoft Office SharePoint Online 2013

### Access privileges for SharePoint scans

To perform the SharePoint scan, the user accounts should have sufficient rights to access and browse the SharePoint site content. The user account must also have permission to invoke Web services and permission to obtain the access control list (ACL).

These rights correspond to the lower-level SharePoint permissions "Browse Directories," "Use Remote Interfaces," and "Enumerate Permissions." Refer to the Microsoft SharePoint documentation for more information on SharePoint permissions and permission levels. If the user account does not have the "Enumerate Permissions" right, then the ACL is not obtained for the SharePoint content.

The following permission levels in SharePoint already have these permissions defined:

 Full Control (includes Browse Directories, Use Remote Interfaces, and Enumerate permissions)

- Design (includes Browse Directories and Use Remote Interfaces permissions)
- Contribute (includes Browse Directories and Use Remote Interfaces permissions)

### **About Alternate Access Mapping Collections**

SharePoint requires all URLs used to access a web application to be defined in Central Administration as internal or public, and the Symantec SharePoint solution expects the user to provide one of those defined URLs as a scan target. Use SharePoint's Alternate Access Mapping Collection to define the web application URLs you use for scanning. For information about configuring Alternate Access Mapping Collections, see

http://technet.microsoft.com/en-us/library/cc288609%28office.12%29.aspx.

### Configuring and running SharePoint server scans

Before you run a scan, you must set up a target using the following procedure.

The SharePoint solution must be installed on the Web Front End in a farm.

See "Installing the SharePoint solution on the Web Front Ends in a farm" on page 1281.

To set up a new target for the scan of a SharePoint server

- Click Manage > Discover Scanning > Discover Targets > New Target > Server > SharePoint.
- 2 On the **General** tab, enter the name of this scan target.
- 3 Select the policy groups that contain the policies for this target scan.
- 4 Select the Discover Servers where this target scan can run.
- 5 Select Scheduling options.

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the schedule drop-down list to display additional fields.

Choose Pause Scan between these times to automatically pause scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon for the target entry.

See "Scheduling Network Discover scans" on page 1194.

On the **Scanned Content** tab, enter the credentials for this scan.

You can specify a default user name for access to all SharePoint sites, except those specified using the **Add** editor.

If you specify SharePoint sites with the **Add** editor, you can specify separate credentials for each site.

The user accounts should have "Browse Directories" permissions in SharePoint to perform the scan. To retrieve permissions, the user account needs the "Enumerate Permissions" SharePoint permission level.

See "Access privileges for SharePoint scans" on page 1277.

7 Specify the SharePoint sites to scan.

For each site, enter a target URL to the SharePoint Web application or site collection or site to be scanned. All the items in its child sites and sub sites are scanned.

For a Web application, specify for example: http://www.sharepoint.com:2020

For a site collection, specify for example:

http://www.sharepoint.com:2020/Sites/collection

For a site or sub-site, specify for example:

http://www.sharepoint.com:2020/Sites/mysharepoint/sub/mysite

For the SharePoint site, use the public URL instead of the internal URL.

The Following syntax applies for the URL and credentials on each line.

```
URL, [username, password]
```

Select one of the following methods of entering the location for the SharePoint server:

Uploaded file

Select **Scan Sites From an Uploaded File**. Create and save a plain text file (.txt) listing the servers you want to scan. Create the file using an ASCII text editor and enter one URL per line. Then click **Browse** to locate the file with the list. Click **Upload Now** to import it.

Individual entries

Select **Scan Sites**. Click **Add** to use a line editor to specify the servers you want to scan. Server information that is entered here takes precedence over the default values and applies only to the path specified.

8 Under Scan Type, select Scan only new or modified items (incremental scan). This option is the default for new targets.

If you have changed the policy or other definitions in an existing scan, you can set up the next scan as a full scan. Select the following option:

Scan all items for the next scan. Subsequent scans will be incremental.

If you always want to scan all items in this target, select the following option:

#### Always scan all items (full scan)

9 On the **Filters** tab, select path filters.

> Use the Include Filter and Exclude Filter to specify the items that Symantec Data Loss Prevention should process or skip. If the field is empty, Symantec Data Loss Prevention performs matching on all items. If you enter any values for the Include Filter, Symantec Data Loss Prevention scans only those items that match your filter. Delimit entries with a comma, but do not use any spaces.

You can provide filters using regular expressions, or paths relative to the location of the SharePoint site. Filters can include a site collection, site, subsite, folder, file name, or file extension. Path filters are not applied on attachments of an item, such as a .doc attachment to a list item.

All path filters are case-sensitive.

For the **Include Filter**, regular expression matching is applied to files, but not to folders.

For the **Exclude Filter**, regular expression matching is applied to both files and folders.

Only the path until the first "?" or "\*" is considered when a folder or file is matched.

When all the specified path filters are relative, the matching folder is skipped, and the scan statistics do not include the items in the skipped folders.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

10 On the Filters tab, select date filters.

The date filters let you include items from the matching process based on their dates. Any items that match the specified date filters are scanned.

See "Filtering Discover targets by date last accessed or modified" on page 1202.

11 On the Filters tab. select size filters.

The size filters let you exclude items from the matching process based on their size. Symantec Data Loss Prevention includes only the items that match your specified size filters. If you leave this field empty, Symantec Data Loss Prevention performs matching on items or documents of all sizes.

See "Filtering Discover targets by item size" on page 1201.

are bytes, KB (kilobytes), or MB (megabytes).

- 12 Select the Advanced tab for options to optimize scanning. On the Advanced tab, you can configure throttling options and set Inventory Mode for scanning.
  - Throttling Options Specify the maximum number of items to be processed per minute, or specify the maximum number of bytes to be processed per minute. For bytes, specify the unit of measurement from the drop-down list. The options

**Note:** Byte throttling is only applied after the fetch of each item. Therefore, actual network traffic may not exactly match the byte throttling that is set.

Inventory Scanning

Enter the number of incidents to produce before moving on to the next site to scan (a URL from the **Scanned Content** tab). To audit whether confidential data exists on a target, without scanning all of it, set up Inventory Mode for scanning. Setting incident thresholds can improve the performance of scanning by skipping to the next site to scan, rather than scanning everything.

After the incident threshold has been reached, the scanning of this site is stopped, and scanning proceeds to the next site. Because the process is asynchronous, a few more incidents may be created than specified in the incident threshold.

### Installing the SharePoint solution on the Web Front Ends in a farm

To scan a SharePoint target using Network Discover, you must install the Symantec SharePoint solution on the Web Front Ends in a farm.

The SharePoint target running on Network Discover communicates with the SharePoint solution and fetches content after the target is authenticated with SharePoint. You can configure the application to use SSL if secure data transfer is required between the Network Discover and SharePoint servers.

Specific permissions are required for the SharePoint solution installation process.

See "Access privileges for SharePoint scans" on page 1277.

The Symantec SharePoint solution is versioned, and is not backward-compatible. If you are upgrading from Symantec Data Loss Prevention version 11.5 or earlier, you must upgrade your SharePoint solution. Table 62-2 lists the SharePoint Solution version that is compatible with your version of Symantec Data Loss Prevention.

**Table 62-2** Symantec SharePoint Solution version compatibility

Symantec SharePoint Solution version	Compatible Symantec Data Loss Prevention versions
No version number	11.0 through 11.5
11.5.1	11.5.1
11.6	11.6, 11.6.1, 11.6.2
12.0	12.0, 12.0.1
12.5	12.5

#### To install the Symantec SharePoint solution

- Copy the SharePoint solution installer Symantec DLP Solution 12.5.exe to a temporary directory on the SharePoint Web Front End. This file is located in the DLP Home\Symantec DLP\_12.5\_Win\Third\_Party\SharePoint or DLP Home/Symantec DLP 12.5 Lin/Third Party/SharePoint directory, where DLP Home is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.
- Start the Windows SharePoint Services Administration service on the SharePoint server. On the SharePoint server, click Start > All Programs > Administrative Tools > SharePoint Central Administration.
- Double-click the Symantec DLP Solution 12.5.exe file. The Symantec Data Loss Prevention solution installation program starts.
- Click **Next**, and the installation program performs a number of preliminary checks.
  - If one of these checks fail, correct the problem and restart the installation program.
  - Click Next.
- 5 Accept the Symantec License Agreement, and click **Next**.

- The installation program copies the files and deploys the solution to all Web Applications in the SharePoint farm.
- 7 After installation, verify that the SharePoint solution has been correctly deployed to the server or server farm.
- Connect to **SharePoint Central Administration**. On the SharePoint server, go to Start > All Programs > Administrative Tools > SharePoint Central Administration.
- 9 For SharePoint 2007, click the Operations tab. In the Global Configuration section, select Solution management.
- 10 For SharePoint 2010, click System Settings. Then select Manage Farm Solutions.
- 11 Verify the deployment. If the solution is installed correctly, the list includes symantec\_dlp\_solution.wsp.
- 12 If the solution must be removed, use the SharePoint retract and undeploy features.

### Setting up SharePoint scans to use Kerberos authentication

A SharePoint scan can optionally use Kerberos authentication.

SharePoint must already be set up to work with Kerberos authentication.

The Discover Server must then be configured to communicate with the Key Distribution Center (KDC) and the SharePoint server.

#### To configure the Discover Server for Kerberos authentication

- Create a file named krb5.conf which contains the realm and the KDC information. On Windows, this file is usually named krb5.ini. A sample file is in the folder C:\SymantecDLP\Protect\config (in a Windows default Symantec Data Loss Prevention installation).
  - See "Creating the configuration file for Active Directory integration" on page 106.
- 2 Copy this file to the Discover Server into the folder C:/SymantecDLP/jre/lib/security/ (in a Windows default Symantec Data Loss Prevention installation).

3 Update the default realm and directory server parameters (realms) in this file.

```
[libdefaults]
    default realm = ENG.COMPANY.COM
[realms]
ENG.COMPANY.COM = {
    kdc = engADserver.emg.company.com
    }
    MARK.COMPANY.COM = {
    kdc = markADserver.emg.company.com
```

See "Creating the configuration file for Active Directory integration" on page 106.

On the Discover Server, update the Protect.properties file in the folder C:\SymantecDLP\Protect\config (in a Windows default Symantec Data Loss Prevention installation). Update the property that points to the updated krb5.ini file.

```
# Kerberos Configuration Information
java.security.krb5.conf=C:/SymantecDLP/jre/lib/security/krb5.ini
```

### **Troubleshooting SharePoint scans**

Table 62-3 provides suggestions for troubleshooting issues with SharePoint scans.

**Table 62-3** Troubleshooting SharePoint scans

Issue	Recommended steps
If an internal SharePoint URL is specified, only the default site collection is scanned.	Specify the public URL for the SharePoint site. All the site collections are scanned.
No site collections, or only the default site collection, are scanned when the Discover Server and SharePoint site are in different domains.	Specify the site collection/site/web application URL with a fully qualified domain name.  To validate the access from the Discover Server, try to access the SharePoint URL from a browser. If a short name does not work, try to use the fully qualified domain name.  Only the default site collection is scanned if the web application URL does not contain fully qualified domain name.

Troubleshooting SharePoint scans (continued) **Table 62-3** 

Issue	Recommended steps
The bytes reported as scanned does not	To improve performance, the scan statistics do not include items in the folders that are skipped (filtered out).
match the number of bytes in the content.	Dynamic content, such as .aspx files, can change size.
,	You can set the Advanced Server setting
	Discover.countAllFilteredItems to get more accurate
	scan statistics.
	See "Advanced server settings" on page 203.

# Setting up scans of Exchange servers

#### This chapter includes the following topics:

- Setting up server scans of 2007 repositories using the Exchange Web Store connector
- About scans of Exchange 2007 servers
- Supported Exchange Server Web Store connector targets
- Providing access rights to scan all mailboxes and public folders
- Configuring Exchange 2007 server scans
- Example configurations and use cases for Exchange 2007 scans
- Troubleshooting Exchange 2007 scans
- Setting up server scans of Exchange 2007 SP2 and 2010 repositories using Exchange Web Services
- About scans of Exchange 2007 SP2 and 2010 servers
- Supported Exchange Server Web Services connector targets
- Configuring Exchange 2007 SP2 and 2010 Server scans
- Example configurations and use cases for Exchange 2007 SP2 and 2010 scans
- Troubleshooting Exchange 2007 SP2 and 2010 scans

### Setting up server scans of 2007 repositories using the Exchange Web Store connector

You can scan Exchange 2007 SP2 and earlier servers using the Exchange Web Store connector. To set up scanning of Exchange 2007 servers using the Exchange Web Store connector, complete the following process:

**Table 63-1** Setting up an Exchange server scan

Step	Action	Description
1	Verify that your Exchange server provides Outlook Web Access and enable WebDAV.	
2	If you need secure access between the Discover Server and your Exchange server or LDAP server, set up HTTPS and LDAPS.	See "Configuring Exchange 2007 server scans" on page 1289.
3	If you want to scan all mailboxes and public folders, make sure to grant access rights for the specific user. The user also needs access to the domain controller.	See "Providing access rights to scan all mailboxes and public folders" on page 1289.
4	Go to Manage > Discover Scanning > Discover Targets to create an Exchange target and to configure scans of Exchange servers.	See "Configuring Exchange 2007 server scans" on page 1289.
5	Set any additional scan options for the Exchange target.	See "Network Discover scan target configuration options" on page 1191.
6	Start the Exchange server scan.	Go to Manage > Discover Scanning > Discover Targets.  Select the scan target from the target list, then click the Start icon.
7	Verify that the scan is running successfully.	See "Managing Network Discover target scans" on page 1209.

### **About scans of Exchange 2007 servers**

The Network Discover Server locates a range of exposed confidential data on Exchange servers, including email messages, calendar items, contacts, journal, and flagged items.

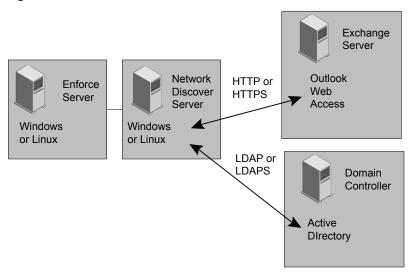
Communication is secure when the Exchange server is configured to use SSL (HTTPS). Communication with the LDAP server is secure when it is configured to use LDAPS.

For HTTPS, validation of the server SSL certificate is not the default. To enable validation of the server SSL certificate, turn on the advanced setting Discover.ValidateSSLCertificates. Then import the server SSL certificate to the Discover Server.

See "Advanced server settings" on page 203.

See "Importing SSL certificates to Enforce or Discover servers" on page 197.

Exchange scan configuration Figure 63-1



### Supported Exchange Server Web Store connector targets

The Exchange Web Store connector supports the following Exchange Server targets:

Microsoft Exchange Server 2007 SP2 or earlier For Exchange 2007 SP2 servers, you can either use the Exchange Web Store connector or Exchange Web Services connector.

To use the Exchange Web Store connector, Outlook Web Access must be configured, and WebDAV must be enabled.

The Exchange scan includes email message text and email file attachments from the user's mailbox.

You can scan the data objects that are stored within Public Folders, such as:

- Email messages
- Message attachments
- Microsoft Word documents
- Excel spreadsheets

The Exchange scan does not target mail stored in Personal Folders (.pst files) or offline folders (.ost files) that are not on the Exchange server. To scan .pst files on a file share, use the shared file system target.

See "Configuring scans of Microsoft Outlook Personal Folders (.pst files)" on page 1253.

### Providing access rights to scan all mailboxes and public folders

If you want to scan all mailboxes and public folders, make sure to grant access rights for the specific user.

Basic, NTML, and form-based authentication is supported. Kerberos is also supported, if it is installed.

#### For Exchange 2007, set up access rights to all mailboxes and public folders

In the Exchange console, run the following to enable access to all mailboxes:

```
Get-Mailbox | Add-MailboxPermission -User specific user
  -Accessright Fullaccess -InheritanceType All
```

- The access to public folders should be enabled by default. Verify the access.
- 3 Restart the Microsoft Exchange Information Store service to propagate the changes immediately.

Note: The changes propagate automatically, but may take 15 minutes or longer.

### **Configuring Exchange 2007 server scans**

Before you run a scan, you must set up a target using the following procedure.

If you want secure access from the Discover Server to the Exchange server, then set up the Exchange server for HTTPS. If you want secure access from the Discover Server to the Domain Server, then set up the Domain Server for LDAPS. Use the same procedure for the Enforce Server, and for each Discover Server that scans an Exchange Server.

See "Importing SSL certificates to Enforce or Discover servers" on page 197.

Note: The "eml" string is special for Exchange server scanning because the files in Exchange have an .eml extension. Review your policies, such as file matching, and avoid using "eml" in the matching for Exchange scans. Also avoid this string in the include or exclude filters of the Exchange scans.

#### To set up a new target for the scan of an Exchange server

- Go to Manage > Discover Scanning > Discover Targets > New Target > Server > Exchange.
- 2 On the **General** tab, enter the name of this scan target.
- 3 Select the policy groups that contain the policies for this target scan.
- 4 Select the Network Discover Servers where this target scan can run.
- 5 Select Scheduling options.

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the schedule drop-down list to display additional fields.

Choose Pause Scan between these times to automatically pause scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon for the target entry.

See "Scheduling Network Discover scans" on page 1194.

On the **Scanned Content** tab, enter the credentials for this scan. 6

All Exchange user names must include the domain name, for example:

```
DOMAIN NAME\user name
```

You can specify a default user name for access to the Exchange site.

See "Providing the password authentication for Network Discover scanned content" on page 1196.

Enter a target URL for the Exchange server to be scanned.

Note: Only one Exchange server can be specified per Discover target.

Select one of the following methods of entering the items to scan on the Exchange server:

#### All users on Directory Server

To use this option, select a Directory Server connection you have already specified, or click the Create new Directory Connection link to configure a new directory connection.

See "Configuring directory server connections" on page 127.

#### Directory groups and users

If directory user groups are available, then select the groups to include in this target.

To use this option, directory groups must be established. If no directory groups are set up, click the link Create new User Group to jump to the page to configure the directory user groups.

See "Configuring User Groups" on page 654.

#### Specify User Mailboxes to include in this Target

Enter specific mailboxes. Alphanumeric characters and the following special characters are allowed in mailbox names:

```
! # $ ' - ^ ` { }
```

You can combine this option with directory groups and users. No directory groups are needed for the user mailboxes option.

#### Public folders

Select this option to scan all public folders on the Exchange server. The user of the credentials that are specified must have access to these public folders.

You can select this option in addition to All users on a Directory Server or Directory groups and users.

#### On the **Filters** tab, select path filters.

Use the Include Filter and Exclude Filter to specify the items that Symantec Data Loss Prevention should process or skip. If the field is empty, Symantec Data Loss Prevention performs matching on all items. If you enter any values for the Include Filter, Symantec Data Loss Prevention scans only those items that match your filter. Delimit entries with a comma, but do not use any spaces.

You can provide filters using regular expressions, or paths relative to the location of the Exchange site. Filters can include a folder name or file name. All path filters are case-sensitive.

Exchange may append an email identifier to the end of the path. To match the filter, add a wildcard to the end. For example to filter for "sample public folder item" use the following filter:

```
*/folder/*/*sample public folder item*
```

You can provide filters using regular expressions, or paths relative to the location of the Exchange site. Filters can include a site collection, site, sub site, folder, file name, or file extension. All path filters are case-sensitive.

For the Include Filter, regular expression matching is applied to files, but not to folders.

For the Exclude Filter, regular expression matching is applied to both files and folders.

Only the path until the first "?" or "\*" is considered when a folder or file is matched.

When all the specified path filters are relative, the matching folder is skipped, and the scan statistics do not include the items in the skipped folders.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

#### 9 On the **Filters** tab, select size filters.

The size filters let you exclude items from the matching process based on their size. Symantec Data Loss Prevention includes only the items that match your specified size filters. If you leave this field empty, Symantec Data Loss Prevention performs matching on items of all sizes.

See "Filtering Discover targets by item size" on page 1201.

**10** On the **Filters** tab, select a Differential scan (optional).

Select Only Scan files added or modified since the last full scan to have Symantec Data Loss Prevention scan only the items or the documents that have been added or modified since the last full scan. The first scan has to be a full (initial base) scan. A full scan occurs if you select this option before Symantec Data Loss Prevention scans this target for the first time.

11 Select Date Filters.

The date filters let you include items from the matching process based on their dates. Any items that match the specified date filters are scanned.

See "Filtering Discover targets by date last accessed or modified" on page 1202.

- 12 Select the Advanced tab for options to optimize scanning. On the Advanced tab, you can configure throttling options and set Inventory Mode for scanning.
  - Throttling Options Specify the maximum number of items to be processed per minute, or specify the maximum number of bytes to be processed per minute. For bytes, specify the unit of measurement from the drop-down list. The options are bytes, KB (kilobytes), or MB (megabytes).
  - Inventory Scanning Enter the number of incidents to produce before completing this scan. To audit whether confidential data exists on a target, without scanning all of it. set up Inventory Mode for scanning.

After the incident threshold has been reached, the scanning is stopped. Because the process is asynchronous, a few more incidents may be created than specified in the incident threshold.

### Example configurations and use cases for Exchange 2007 scans

Table 63-2 lists the options to select on the **Scanned Content** tab during the configuration of an Exchange target.

Exchange 2007 scan use cases **Table 63-2** 

Use case	Description
Scan all user mailboxes and public folders.	Select the following options in the user interface:  All users on Directory Server  Public folders
	The credentials must include a user who has access to the mailboxes, and also access to the domain controller (to retrieve the list of users).
	See "Providing access rights to scan all mailboxes and public folders" on page 1289.
Scan all users mailboxes	Select the option All users on Directory Server in the user interface.
(but not public folders).	The credentials must include a user who has access to the mailboxes, and also access to the domain controller (to retrieve the list of users).
	See "Providing access rights to scan all mailboxes and public folders" on page 1289.
Scan all public folders.	Select the <b>Public folders</b> option in the user interface.
	The credentials must include a user who has access to the public folders.
Scan all user mailboxes	Select the <b>Directory groups and users</b> option in the user interface.
belonging to a specified group.	Then select the Directory Group from the groups in the list. All user mailboxes in the group are scanned.
	The credentials must include a user who has access to the mailboxes, and also access to the domain controller (to retrieve the list of users).
	See "Providing access rights to scan all mailboxes and public folders" on page 1289.
Scan an individual user	Select the <b>Directory groups and users</b> option in the user interface.
mailbox.	Then enter the individual user mailbox name.
	The credentials must include access for the specified user mailbox.
Scan the user mailboxes	On the Exchange server, the user mailboxes may be in a different store than the default.
that are not on the default store for Exchange.	Specify the Exchange URL containing the path to the alternate store, credentials with access to the mailboxes, and the mailboxes to scan using any of the methods in this table.
Scan the public folders that	On the Exchange server, the public folders may be in a different store than the default.
are not on the default store for Exchange.	Specify the Exchange URL containing the path to the public folders and credentials with access to the public folders.
	Select the <b>Public folders</b> option in the user interface.

### **Troubleshooting Exchange 2007 scans**

Table 63-3 provides suggestions for troubleshooting issues with Exchange scans.

Troubleshooting Exchange 2007 scans **Table 63-3** 

Issue	Recommended steps	
A mailbox is created, but never logged on. The mailbox is not scanned.	Log on to the mailbox. Then the mailbox is scanned.	
In the Exchange logs, the user that scanned the Exchange server is reported as "Last Logged on By" in the user activity.	This log entry indicates the last user to use the mailbox, which may be the user that scanned it.	
The bytes reported as scanned do not match the	To improve performance, the scan statistics do not include items in the folders that are skipped (filtered out).	
number of bytes in the content.	You can set Discover.countAllFilteredItems in Server Detail > Advanced Server Settings to get more accurate scan statistics.	
	See "Advanced server settings" on page 203.	
The connection to the Exchange server times out,	The default value for the timeout of the connection to the Exchange server is five minutes (300000 milliseconds).	
and no items are scanned.	To increase the value, add and set the property in the configuration file crawler.properties. For example, to set the timeout to 10 minutes, add or modify the following line:	
	crawler.exchange.serverTimeout = 600000	
All items trigger incidents if the file type detection rule is set to detect Outlook Express items in the policy for an Exchange scan.	Remove Outlook Express from the file type detection rule.	

### Setting up server scans of Exchange 2007 SP2 and 2010 repositories using Exchange Web Services

You can crawl Exchange 2007 SP2 (and later) and 2010 Servers using Exchange Web Services.

**Table 63-4** Setting up an Exchange server scan

Ston	Action	Description
Step	Action	Description
1	Verify that Exchange Web Services and the Autodiscover Service are enabled on your Exchange server and are accessible from the Network Discover server.	For information about Exchange Web Services and the Autodiscover service, see your Microsoft Exchange documentation.
2	If you need secure access between the Discover Server and Exchange Web Services or your Active Directory server, set up HTTPS and LDAPS.	By default, Symantec Data Loss Prevention only allows HTTPS connections to the Active Directory server and Exchange Web Services. To allow HTTP connections, set the  Discover.Exchange.UseSecureHttpConnections setting in Server Detail > Advanced Server Settings to false.  See "Advanced server settings" on page 203.
3	Ensure that your Exchange user credentials can impersonate any mailbox you want to scan.	For information about enabling impersonation for your user credentials, see your Microsoft Exchange documentation.
4	Go to Manage > Discover Scanning > Discover Targets to create an Exchange target and to configure scans of Exchange servers.	See "Configuring Exchange 2007 SP2 and 2010 Server scans" on page 1298.
5	Set any additional scan options for the Exchange target.	See "Network Discover scan target configuration options" on page 1191.
6	Start the Exchange server scan.	Go to Manage > Discover Scanning > Discover Targets.  Select the scan target from the target list, then click the Start icon.
7	Verify that the scan is running successfully.	See "Managing Network Discover target scans" on page 1209.

### About scans of Exchange 2007 SP2 and 2010 servers

You can scan Exchange 2007 SP2 (and later) and 2010 servers using the Exchange Web Services connector. For Exchange 2007 SP2 servers, you can either use the Exchange Web Store connector or the Exchange Web Services connector. The Exchange Web Services connector does not require an agent on the Exchange server, and it does not search every Exchange server. Using the Exchange Autodiscover feature, it fetches Exchange server and mailbox information from Active Directory, and pulls data directly from the appropriate Exchange servers

using the Simple Object Access Protocol (SOAP). For more information on the Exchange Autodiscover feature, see

http://technet.microsoft.com/en-us/library/bb124251.aspx.

The Network Discover Server locates a range of exposed confidential data on Exchange servers, including email messages, calendar items, contacts, journal, and flagged items.

Communication is secure when the Exchange server is configured to use SSL (HTTPS). Communication with the Active Directory server is secure when it is configured to use LDAPS.

For HTTPS, validation of the server SSL certificate is not the default. To enable validation of the server SSL certificate, turn on the advanced setting Discover.ValidateSSLCertificates. Then import the server SSL certificate to the Discover Server.

By default, Network Discover uses secure connections to the Exchange and Active Directory servers. You can disable secure access to Exchange and Active Directory by setting the Discover. Exchange. UseSecureHttpConnections setting in Server **Detail > Advanced Server Settings to false.** 

See "Advanced server settings" on page 203.

See "Importing SSL certificates to Enforce or Discover servers" on page 197.

Note: Network Discover does not support scans of Exchange targets using Dynamic Distribution Groups.

## Supported Exchange Server Web Services connector targets

The Exchange Web Services connector supports the following Exchange Server targets:

- Microsoft Exchange Server 2007 SP2 or later For Exchange 2007 SP2 servers, you can either use the Exchange Web Services connector or the Exchange Web Store connector.
- Microsoft Exchange Server 2010

To use the Exchange Web Services connector, Exchange Web Services and the Autodiscover Service must be enabled on your Exchange server and are accessible to the Network Discover server.

You can scan the data objects that are stored within Public Folders, such as:

- Email messages
- Message attachments
- Microsoft Word documents
- Excel spreadsheets

The Exchange scan also targets mail stored in Exchange 2010 Personal Archives.

## Configuring Exchange 2007 SP2 and 2010 Server scans

Before you run a scan, you must set up a target using the following procedure.

To set up a new target for the scan of an Exchange server using Exchange Web Services

- 1 Go to Manage > Discover Scanning > Discover Targets > New Target > Server > Exchange.
- 2 On the **General** tab, enter the name of this scan target.
- 3 Select the policy groups that contain the policies for this target scan.
- 4 Select the Network Discover Servers where this target scan can run.
- 5 Select Scheduling options.

Choose Submit Scan Job on Schedule to set up a schedule for scanning the specified target. Select an option from the schedule drop-down list to display additional fields.

Choose **Pause Scan between these times** to automatically pause scans during the specified time interval. You can override a target's pause window by going to the Discover Targets screen and clicking the start icon for the target entry. The pause window remains intact, and any future scans that run up against the window can pause as specified. You can also restart a paused scan by clicking the continue icon for the target entry.

See "Scheduling Network Discover scans" on page 1194.

6 On the **Scanned Content** tab, enter the credentials for this scan.

All Exchange user names must include the domain name, for example:

```
DOMAIN NAME\user name
```

Ensure that the user credentials you provide can impersonate all mailboxes you want to scan. For information about configuring Exchange Impersonation, see http://msdn.microsoft.com/en-us/library/bb204095%28v=exchg.80%29.aspx.

See "Providing the password authentication for Network Discover scanned content" on page 1196.

7 Enter a target URL for the Microsoft Active Directory server. For example, Idaps://dc.domain.com:636.

Note: Only one Active Directory server can be specified per Discover target.

Select **Public folders** to scan all public folders on the Exchange server. The user of the credentials that are specified must have access to these public folders.

Note: In mixed Exchange environments where both Exchange 2007 and 2010 servers are deployed, Network Discover only scans the public folders from the version specified by the credentials you entered in the Exchange Network Discover target. To scan public folders across both versions 2007 and 2010 in mixed environments, create a separate Network Discover target for each version.

You can select this option in addition to All users on a Directory Server or Directory groups and users.

- Select Mailboxes to scan user mailboxes on your Exchange servers. Select 9 one of the following methods of entering the items to scan on the Exchange server:
  - All users on Directory Server

If a directory server is available, then select the **Directory Server** from the drop-down list.

To use this option, select the Directory Server connection you have already specified, or click the Create new Directory Connection link to configure another directory connection.

See "Configuring directory server connections" on page 127.

Directory groups and users

If directory user groups are available, then select the groups to include in this target.

To use this option, directory groups must be established. If no directory groups are set up, click the link Create new User Group to jump to the page to configure the directory user groups.

See "Configuring User Groups" on page 654.

#### Specify User Mailboxes to include in this Target

Enter specific mailboxes. Alphanumeric characters and the following special characters are allowed in mailbox names:

```
! # $ ' - ^ ` { }
```

You can combine this option with directory groups and users. No directory groups are needed for the user mailboxes option.

#### Personal Archives

Select this option to scan Exchange 2010 Personal Archive mailboxes for the users you have specified.

### 10 On the **Filters** tab, select path filters.

Use Include Filters and Exclude Filters to specify the items that Symantec Data Loss Prevention should process or skip. If the field is empty, Symantec Data Loss Prevention performs matching on all items. If you enter any values for the Include Filter, Symantec Data Loss Prevention scans only those items that match your filter. Delimit entries with a comma, but do not use any spaces.

You can provide filters using regular expressions, or paths relative to the location of the Exchange site. Filters can include a folder name or file name. All path filters are case-sensitive.

Exchange may append an email identifier to the end of the path. To match the filter, add a wildcard to the end. For example to filter for "sample public folder item" use the following filter:

```
*/folder/*/*sample public folder item*
```

You can provide filters using regular expressions, or paths relative to the location of the Exchange site. Filters can include a site collection, site, sub site, folder, file name, or file extension. All path filters are case-sensitive.

For **Include Filters**, regular expression matching is applied to files, but not to folders.

For Exclude Filters, regular expression matching is applied to both files and

Only the path until the first "?" or "\*" is considered when a folder or file is matched.

When all the specified path filters are relative, the matching folder is skipped, and the scan statistics do not include the items in the skipped folders.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

#### 11 On the Filters tab, select size filters.

The size filters let you exclude items from the matching process based on their size. Symantec Data Loss Prevention includes only the items that match your specified size filters. If you leave this field empty, Symantec Data Loss Prevention performs matching on items of all sizes.

See "Filtering Discover targets by item size" on page 1201.

12 On the **Filters** tab, select a differential scan (optional).

Select Only Scan files added or modified since the last full scan to have Symantec Data Loss Prevention scan only the items or the documents that have been added or modified since the last full scan. The first scan has to be a full (initial base) scan. A full scan occurs if you select this option before Symantec Data Loss Prevention scans this target for the first time.

13 Select Date Filters.

The date filters let you include items from the matching process based on their dates. Any items that match the specified date filters are scanned.

See "Filtering Discover targets by date last accessed or modified" on page 1202.

14 Select the Advanced tab for options to optimize scanning. On the Advanced tab, you can configure throttling options and set Inventory Mode for scanning.

#### Throttling Options

You can use throttling to limit the bandwidth consumed by your scan, or to limit the load on your Exchange server. Specify the maximum number of items to be processed per minute, or specify the maximum number of bytes to be processed per minute. For bytes, specify the unit of measurement from the drop-down list. The options are bytes, KB (kilobytes), or MB (megabytes).

#### Inventory Scanning

Enter the number of incidents to produce before completing this scan. To audit whether confidential data exists on a target, without scanning all of it, set up inventory mode for scanning.

After the incident threshold has been reached, the scanning is stopped. Because the process is asynchronous, a few more incidents may be created than specified in the incident threshold.

## Example configurations and use cases for Exchange 2007 SP2 and 2010 scans

Table 63-5 lists the options to select on the **Scanned Content** tab during the configuration of an Exchange target.

Ensure that the user credentials you provide can impersonate all mailboxes you want to scan. For information about configuring Exchange Impersonation, see http://msdn.microsoft.com/en-us/library/bb204095%28v=exchg.80%29.aspx.

Table 63-5	Exchange 200	7 SP2 and	d 2010 scan	use cases
------------	--------------	-----------	-------------	-----------

Use case	Description	
Scan all user mailboxes and public folders.	Select the following options in the user interface:	
	<ul> <li>Public folders</li> <li>Mailboxes &gt; All users on Directory Server</li> </ul>	
	The credentials must have permission to impersonate all mailboxes you want to scan.	
Scan all user mailboxes (but	Select Mailboxes > All users on Directory Server in the user interface.	
not public folders).	The credentials must have permission to impersonate all mailboxes you want to scan.	
Scan all public folders.	Select <b>Public folders</b> in the user interface.	
Scan specific groups or	Select Mailboxes > Directory groups and users in the user interface.	
users.	To scan a Directory Group, select the Directory Group from the groups in the list. All user mailboxes in the group are scanned. You can click <b>Create new User Group</b> to create a new Directory Group.	
	To scan for specific users, enter a comma-separated list of user mailbox names.	
	The credentials must have permission to impersonate all mailboxes you want to scan.	
Scan an Exchange 2010 Personal Archive.	Select Mailboxes > All users on Directory Server > Personal Archives or Mailboxes > Directory groups and users > Personal Archives in the user interface. If necessary, specify which mailboxes to scan. Network Discover scans the Personal Archives associated with the specified mailboxes.	

## **Troubleshooting Exchange 2007 SP2 and 2010 scans**

If you experience problems with Exchange 2007 SP2 and 2010 scans, you can look for more information here:

■ FileReader0.log: This file logs all SOAP requests and responses between Network Discover and Exchange Web Services.

To configure the file reader log to list SOAP requests, edit the FileReaderLogging.properties file as follows:

```
java.util.logging.FileHandler.level = FINEST
org.apache.cxf.interceptor.LoggingInInterceptor.level = FINEST
net.entropysoft.eci.exchangewebservices.schema.SchemaHelper.level = WARNING
net.entropysoft.eci.exchangewebservices.schema.PropertyManagersReader.level = WARNING
org.apache.commons.beanutils.converters.level = WARNING
net.entropysoft.eci.exchangewebservices.AutodiscoverHelper.level = FINEST
net.entropysoft.eci.exchangewebservices.ExchangeWebServicesHelper= FINEST
net.entropysoft.eci.exchangewebservices.level = FINE
```

See "Operational log files" on page 244.

Note: Only the java.util.logging.FileHandler.level = FINEST line is present. You must add the others as specified in the above example.

■ Exchange logs: You might find useful troubleshooting information in the logs created by your Microsoft Exchange Server.

# About Network Discover scanners

This chapter includes the following topics:

- Setting up scanning of Microsoft Exchange Servers
- How Network Discover scanners work
- Troubleshooting scanners
- Scanner processes
- Scanner installation directory structure
- Scanner configuration files
- Scanner controller configuration options

## Setting up scanning of Microsoft Exchange Servers

The Exchange Scanner is a stand-alone utility that lets you extract data from Microsoft Exchange and send the data to Network Discover for content processing.

The Exchange scanner accesses client mailboxes on the Exchange server using a connected Outlook client.

The Exchange scanner lets you specify which MAPI profile should be used to extract data from the Exchange structure. The Exchange scanner uses Profiles to connect to the Exchange Server through the MAPI interface. It then posts the files to Discover.

You can use the Exchange Scanner to perform the following tasks:

Scan public folders using a specific account to find the confidential data.

- Scan all the mailboxes using an Administrator account that can access all the mailboxes.
- Scan a particular user's mailbox using the Administrator account.
- Scan a single user's mailbox, with the user name and password known.

To set up scanning of Microsoft Exchange Servers, complete the following process:

Setting up an Exchange scanner **Table 64-1** 

Step	Action	Description
1	Verify that your Exchange server is either version 2003 or 2007.	
2	Install the Exchange scanner on any computer that has Microsoft Outlook 2003 or 2007 installed and a valid Outlook profile configured.	
3	Configure the ProfileName, and the setting for DNMailbox.	
4	Perform any manual configurations by editing the configuration files and properties files.	
5	On the Enforce Server, add a new Exchange target.	See "Adding a new Network Discover target" on page 1187.
6	Start the Exchange scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See "Starting file system scans" on page 1319.
7	Verify that the scan is running successfully.	See "Troubleshooting scanners" on page 1307.

### How Network Discover scanners work

Scanners are the standalone applications that collect content and metadata from a repository and send them to Network Discover for processing.

For example, in a two-tier configuration you might have an Enforce Server and a Network Discover Server that is connected to a Documentum server with a scanner installed.

You can perform the following tasks on the computers in this configuration:

On the Enforce Server, define the scan target (in this example, Documentum).

- On the Documentum server, install the Documentum scanner, configure the scanner to post content to the Network Discover Server, and start (or stop) a scanner.
- On the Enforce Server, start or stop a target scan (with the Start icon), and view the incident reports.

The scanner system communicates with the Network Discover Server using the HTTP protocol.

When the scanner runs, it performs following tasks:

- Natively connects to the repository, and crawls the repository to read the content and metadata.
- Extracts the text and some metadata.
- Posts this extracted information to the Network Discover Server.
- Network Discover consumes the text and metadata and applies detection.

See "About Network Discover" on page 1180.

## **Troubleshooting scanners**

After a scan is started, it extracts content and metadata from the repository. Then it passes this content to the Scan Controller and the Network Discover Server.

See "How Network Discover scanners work" on page 1306.

If a scanner does not seem to be processing items, use the following suggestions:

Table 64-2 Scanner troubleshooting suggestions

Issue	Suggestions
Scanner does not seem to be running.	Verify that the scanner was installed properly.  On the system where the scanner is installed, make sure that the scanner processes are running.  See "Scanner processes" on page 1309.
Incidents do not appear in the reports.	Verify that the scan target is set up properly. Scanners can only send content to a target of the same type. Multiple scanners of the same type can feed content to a Network Discover scan of that type.  Check that the scan is not stalled.

Scanner troubleshooting suggestions (continued) **Table 64-2** 

Issue	Suggestions		
The scan does not seem to	Look in the outgoing folder.		
start.	See "Scanner installation directory structure" on page 1309.		
	If a given scanner cannot send content to Network Discover, that content queues up in the outgoing folder.		
	Items that appear and disappear from this folder indicate normal progress.		
The scan appears stalled.	If a scanner cannot send content to Network Discover, the scanner content queues up on the scanner system. The scanner system must have access to the Network Discover Server. System warnings such as low disk space or down services should be in place on both systems before installation.		
	To verify received content on the Network Discover Server, view the scan statistics page of the scan. To view scan statistics, click on the running scan in the target scan list.		
	Verify that scan information moves through the scan process by checking the logs and temporary directories.		
	See "Scanner installation directory structure" on page 1309.		
	If the scan appears stalled, check the following locations on the scanner computer to diagnose the problem:		
	■ The /logs folder		
	The /scanner_typeScanner/logs folder has the scanner start, stop, and connection status to Network Discover. Similar information is in the Console Window. Check the log files to verify that a scanner is running successfully.		
	■ The /failed folder		
	Items that appear in the /failed folder indicate a mismatch of the scanner types, between the New Target and the scanner. For example if an Exchange scanner is specified in the New Target, but the scanner is SharePoint, then items appear in the /failed folder.		
	■ The /outgoing folder		
	Items that appear and disappear from this folder indicate normal progress. If items linger in this folder and are not consumed (do not disappear), a problem in extracting text and metadata is indicated.		
	If a given scanner cannot send content to Network Discover, that content queues up in the /outgoing folder.		
	■ The /scanner_typeScanner/scanner directory has the scanner connection status to the repository, repository crawling information, and fetched data.		

## Scanner processes

Table 64-3 provides the information about Network Discover scanner processes on a Windows operating system.

**Table 64-3** Discover processes

Processes	Executable	Description	
ScannerController	<pre>scanner_typeScanner_Console.exe  or scanner_typeScanner_Service.exe</pre>	Process that configures and controls the connector, sends content to the Network Discover Server, and sends end-of-scan message to Network Discover.	
Connector	scanner_typeScanner.exe	Process that extracts documents and metadata from the repository.	
ImportModule	ImportSlave.exe	Process that extracts text and metadata from the documents that the connector downloaded.	
KeyView	KVoop.exe	The KeyView process does the text extraction and metadata extraction from known document types.	
Binslave	BinSlave.exe	Process that attempts to extract text from unknown document types.	

# Scanner installation directory structure

Table 64-4 describes the directory structure for Network Discover scanner configuration files.

Installation directory structure Table 64-4

Path	Description
/scanner_typeScanner	
/bin	Files to run the scanner, start, and stop it.
/Clean.exe	Cleans all temp files and logs under the /scanner directory.
/EncryptPassword.exe	Can be used to encrypt the user names and passwords that are put in the scanner_typeScanner.cfg file.
/scanner_typeScanner_Console.exe	Launches the scanner as a console application (with a window). Type CTRL+C to stop the scanner.
/scanner_typeScanner_Service.exe	Launches the scanner as an application without a window. Typically, this launch is only used when the scanner is registered and run as a Windows or UNIX service.
/config	Configuration files are in this directory.
/ScannerController.properties	Configuration file for the ScannerController.
/ScannerControllerLogging.properties	Properties file for the Scanner logging.
/scanner_typeScanner.cfg	The configuration file for the connector. This file is copied to the /scanner directory before the child process is launched.
/logs	Contains the log files for the ScannerController process.
/outgoing	XML files that contain content and metadata are queued in this folder before they are sent to the Network Discover Server.
/scanner	Binaries, the log files, and the temp files are under this directory.

Path Description Some connectors (for example ..../outgoing Exchange and SharePoint2003) cannot be configured to write the .idx files to the ./outgoing folder. Instead, they write them to ./scanner/outgoing folder and the ScannerController moves them to the . /outgoing directory so that they can be sent to the Network Discover Server. ..../failed If the Network Discover Server cannot parse the XML and returns a 500 error code, the ScannerController moves the offending XML document to the ./failed folder.

**Table 64-4** Installation directory structure (continued)

# Scanner configuration files

Configuration options can be edited after installation and before you start a scan by editing the following files on the scanner system.

#### File name

#### ScannerController.properties

#### **Configuration Tasks**

In the ScannerController.properties file, you can configure the following options:

- Define Network Discover Server connection information.
- Provide content compression to reduce network load.
- Turn on and off incremental scanning. Additional configuration may be required in the Vontuscanner typeScanner.cfg file.

See "Scanner controller configuration options" on page 1312.

#### File name **Configuration Tasks** ScannerControllerLogging.properties In the ScannerControllerLogging.properties file, you can configure the following options: Specify the logging levels from .level = INFO to .level = FINEST. Vontuscanner typeScanner.cfg In the Vontuscanner typeScanner.cfg file, you can configure the following options: Specify multiple jobs (run sequentially). Define access credentials. See "Encrypting passwords in configuration files" on page 1197. Define filters. Define throttling. Specific settings are also available for each

## Scanner controller configuration options

Initial scanner configuration occurs during installation. Following installation, you can modify or specify additional scan settings.

scanner type.

Table 64-5 provides an explanation of commonly modified parameters in the ScannerController.properties file.

Commonly modified parameters in ScannerController.properties **Table 64-5** 

Parameter	Default	Description
discover.host	localhost	The host name or IP address of the Network Discover Server the scanner routes content to. Before you configure this value, the Network Discover Server should be added to the Enforce Server, and access to it from the scanner verified.
discover.port	8090	The Network Discover port to which the scanner routes data.
discover.compress	true	Specify whether or not to compress content before routing it to the Network Discover Server. Compression reduces network load, but consumes extra CPU on the scanner computer and on the Network Discover Server.

Commonly modified parameters in ScannerController.properties **Table 64-5** (continued)

Parameter	Default	Description
discover.retry.interval	1000	Milliseconds the scanner should wait before it retries to connect to the Network Discover Server after a disconnect or previous failure.
scanner.send.endofscanmarker	true	If this parameter is set to false, the scanner runs until it is stopped manually in the Enforce Server console. The scan restarts from the beginning after it reaches the end of the scan list.
scanner.incremental	false	When true, the scanner only scans documents with created or modified dates after the last complete scan. When false, all files are scanned each time the scan is run.
dre.fake.port	disabled http://localhost:19821	Used only by certain scanners to prevent content from being misdirected to an incorrect process. Must also be modified with values for DREHost and ACIPort in the scanner_typeScanner.cfg file.  The dre.fake.port specifies the port that the ScannerController binds to. It makes sure that the connector does not attempt to send content to some other process.
queue.folder.path	disabled ./scanner/outgoing	Used only for certain scanners to bridge a difference in location between where .idx files are written and where they are expected. This parameter is for the Exchange and SharePoint 2003 scanners.

# Setting up scanning of file systems

#### This chapter includes the following topics:

- Setting up remote scanning of file systems
- Supported file system scanner targets
- Installing file system scanners
- Starting file system scans
- Installing file system scanners silently from the command line
- Configuration options for file system scanners
- Example configuration for scanning the C drive on a Windows computer
- Example configuration for scanning the /usr directory on UNIX
- Example configuration for scanning with include filters
- Example configuration for scanning with exclude filters
- Example configuration for scanning with include and exclude filters
- Example configuration for scanning with date filtering
- Example configuration for scanning with file size filtering
- Example configuration for scanning that skips symbolic links on UNIX systems

## Setting up remote scanning of file systems

Scanning the file systems that are not file shares or servers is accomplished with a multiple computer installation. On the computer with the file system, scanning software sends data to the Network Discover Server for processing.

See "How Network Discover scanners work" on page 1306.

For file shares, use the server file system target.

See "Setting up server scans of file systems" on page 1241.

To set up scanning of file systems, complete the following process:

**Table 65-1** Setting up a file system scanner

Step	Action	Description
1	Verify that your file system is on the list of supported targets.	See "Supported file system scanner targets" on page 1316.
	The file system scanner can scan local file systems on remote Windows, Linux, AIX, and Solaris servers.	
2	On the server that contains the file system, install the file system scanner.	See "Installing file system scanners" on page 1316.
	The setup for scanning file systems requires installation of the scanner software on the computer where the file system is located.	See "Installing file system scanners silently from the command line" on page 1320.
	On Linux, AIX, and Solaris, the root user must install the scanner.	
3	Perform any manual configurations by editing the configuration files and properties files.	See "Configuration options for file system scanners" on page 1321.
4	On the Enforce Server, add a new Scanner File System target.	See "Adding a new Network Discover target" on page 1187.
5	Start the file system scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See "Starting file system scans" on page 1319.
6	Verify that the scan is running successfully.	See "Troubleshooting scanners" on page 1307.

## Supported file system scanner targets

The following remote Windows systems can be scanned:

- Windows Server 2008
- Windows Server 2012

The following Linux file systems can be scanned:

- Red Hat Enterprise Linux 5.x
- Red Hat Enterprise Linux 6.x

The following AIX file systems can be scanned:

- AIX 5.3
- AIX 6.1

AIX requires the following C run time libraries, as well as Java 1.5 and Java 7 JRE:

- xlC.aix50.rte (v8.0.0.0+)
- $\blacksquare$  xlC.rte (v8.0.0.0+)

The following 32-bit Solaris file systems can be scanned (64-bit systems are not supported):

- Solaris 9 (SPARC platform)
- Solaris 10 (SPARC platform)

Solaris requires the following patch levels for the scanner:

Solaris 9, 115697-01 http://sunsolve.sun.com/search/document.do?assetkey=1-21-115697-02-1

File systems on UNIX systems can also be scanned using the SFTP protocol. This protocol provides a method similar to share-based file scanning, instead of using the File System Scanner. Contact Symantec Professional Services for details.

## Installing file system scanners

The File System Scanner must be installed on the computer with the file system you want to scan.

On Linux, AIX, and Solaris, the root user must install the scanner.

If a user other than the one who installed the scanner wants to run it, permissions must be changed. On Linux, AIX, and Solaris, appropriate permissions must be given to the directories and files.

#### To install the file system scanner

On the computer with the file system to scan, download or copy (as binary) the relevant installation file to a temporary directory. The file is located in the DLP Home\Symantec DLP 12 Win\Scanners Of

DLP Home/Symantec DLP 12 Lin/Scanners directory, where DLP Home is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

#### The file is one of the following file names:

- SymantecDLPScanners windows x32 12.5.exe
- SymantecDLPScanners Aix 12.5.sh
- SymantecDLPScanners Unix x32 12.5.sh (for 32-bit Linux systems)
- SymantecDLPScanners Unix x64 12.5.sh (for 64-bit Linux systems)

Note: You can install either the 32-bit or 64-bit scanner on 64-bit Linux systems. We recommend the 64-bit version.

- SymantecDLPScanners Solaris 12.5.sh
- Start the scanner installation program.

Use the -c flag to install a scanner with a console command (rather than with a GUI).

#### Windows GUI:

SymantecDLPScanners windows x32 12.5.exe

#### 32-bit Linux GUI:

./SymantecDLPScanners Unix x32 12.5.sh

#### 32-bit Linux console:

- ./SymantecDLPScanners Unix x32 12.5.sh -c
- 3 If applicable, confirm the version of the scanner you want to install (32-bit or 64-bit).
- Confirm the license ageement.
- 5 Select File System Scanner.
- Select the installation Destination Directory (the directory where you want the SymantecDLP File System Scanner installed).

- 7 For Windows, select the Start Menu Folder (shortcut in the Start menu). The default is SymantecDLP FileSystem Scanner.
- 8 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or host name of the Network Discover Server)
  - Discover Port
- 9 Configure the File System Scanner by entering the following information:
  - Scan Directory List of directories to scan. Delimit with a comma (no space).
  - Path Include Filter Only the paths that include all the string(s) specified here are scanned. Delimit with a comma (no space).
  - Path Exclude Filter Everything but the directories that contain the string(s) specified here are scanned. Delimit entries with a comma, but do not use any spaces. Note that the Include Filter and Exclude Filter file names are relative to the file system root. Specify full paths or subdirectories, as needed.
- 10 The scanner installs.
- 11 Select the Startup Mode.

While you initially test or verify that the scanner runs successfully, do not select either of these options, but start the scanner manually.

You can select one (or none) of the following options:

- Install as a service on a Windows system.
- Start after installation.
- 12 The File Scanner installation is complete on the scanner computer.
- 13 Perform any manual configurations by editing the configuration files and properties files.

See "Configuration options for file system scanners" on page 1321.

See "Scanner installation directory structure" on page 1309.

See "Scanner configuration files" on page 1311.

- 14 On the Enforce Server, create a New Target for the scanner File System type.
- 15 Start the scan on both the scanner computer and the Enforce Server.

See "Starting file system scans" on page 1319.

## Starting file system scans

Make sure that the scanner is installed and configured on the target computer, and a new target is added on the Enforce Server.

See "Installing file system scanners" on page 1316.

Then, you can start the scan.

The procedures are different for each of the following scenarios:

- One scanner per target (first procedure).
- Multiple scanners for one target (second procedure).

#### To start a file system scan with one scanner for one target

Log on to the Enforce Server.

Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- Select the scan target from the target list, then click the Start icon.
- On the scanner computer, start the File System scanner.

On Windows, select Start > Vontu FileSystem Scanner > Vontu FileSystem Scanner Console.

On UNIX, enter the following command:

```
/opt/FileSystemScanner/bin/FileSystemScanner Console
```

The scanner starts the process of scanning data.

See "How Network Discover scanners work" on page 1306.

If the scan does not progress normally, you can troubleshoot it.

See "Troubleshooting scanners" on page 1307.

Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

#### To start a file system scan with multiple scanners for one target

On each of the scanner computers, start the File System scanner on that computer.

On Windows, select Start > Vontu FileSystem Scanner > Vontu FileSystem Scanner Console.

On UNIX, enter the following command:

```
/opt/FileSystemScanner/bin/FileSystemScanner Console
```

Make sure that each of the scanners has started, and has posted information. Check the outgoing folder on each of the computers.

See "Scanner installation directory structure" on page 1309.

2 Log on to the Enforce Server.

> Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- Select the scan target from the target list, then click the Start icon.
- The scanner starts the process of scanning data.
  - See "How Network Discover scanners work" on page 1306.
- 5 If the scan does not progress normally, you can troubleshoot it.
  - See "Troubleshooting scanners" on page 1307.
- Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

## Installing file system scanners silently from the command line

To automate installation, you can preconfigure a text file varfile with your installation choices, and then launch the installation from a command line.

Another method of installing a scanner is with an interactive installation.

See "Installing file system scanners" on page 1316.

#### To automate file scanner installation

- Create a text file, for example FileSystemScanner.varfile.
- 2 Enter your specific parameters, and save the file to the same location as the relevant shell script for your scanner installation.

```
sys.programGroup.allUsers$Boolean=true
discover.host=test-server.test.lab
discover.port=8090
sys.service.selected.417$Boolean=true
job.0.excludeFilters=
sys.languageId=en
sys.programGroup.linkDir=/usr/local/bin
installService$Boolean=false
sys.installationDir=/opt/FileSystemScanner
sys.programGroup.enabled$Boolean=true
job.0.includeFilters=
job.0.directory=/home/text files/text scan/text
sys.service.startupType.417=auto
startAfterInstall$Boolean=false
```

To run the installation with the varfile, type the following command (for Linux):

```
# ./FileSystemScanner Unix 11.6.sh
-varfile FileSystemScanner.varfile -q
```

The parameter -q performs a silent installation.

## Configuration options for file system scanners

Table 65-2 provides a description of the primary parameters in the VontuFileSystemScanner.cfg file.

Parameters in the VontuFileSystemScanner.cfg file **Table 65-2** 

Туре	Parameter	Description
Scanned Content	DirectoryPathCSVs	Comma-separated list of directories to scan.
Scanned Content	DirectoryCantHaveCSVs	Exclude filters of the paths. Delimit entries with a comma, but do not use any spaces.

Table 65-2	Parameters in the VontuFileSystemScanner.cfg file (continued)		
Туре	Parameter	Description	
Scanned Content	DirectoryMustHaveCSVs	Include filters of the paths. Delimit entries with a comma, but do not use any spaces.	
Scanned Content	DirectoryAfterDate	Date filter (in days relative to today).	
Scanned Content	DirectoryBeforeDate	Date filter (in days relative to today).	
Scanned Content	DirectoryFileMatch	For scanning files without an extension on Solaris or Linux systems, set this parameter to the following value:  DirectoryFileMatch=*	
Scanned Content	ImportPreImportMinLength	Minimum size of files.	
Scanned Content	ImportPreImportMaxLength	Maximum size of files.	
Throttling	ImportPoliteness	Specify the amount of time (in milliseconds) that the import module should wait between documents.	
Throttling	PollingMaxNumber	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover.	

See "Optimizing resources with Network Discover scan throttling"

on page 1204.

# Example configuration for scanning the C drive on a Windows computer

Scan the C drive on a Windows computer.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

DirectoryPathCSVs=C:\ DirectoryMustHaveCSVs= DirectoryCantHaveCSVs=

## Example configuration for scanning the /usr directory on UNIX

Scan the /usr directory on a UNIX computer.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

DirectoryPathCSVs=/usr DirectoryMustHaveCSVs= DirectoryCantHaveCSVs=

## **Example configuration for scanning with include** filters

Scan selected files and directories using the include filters.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

Include only the files that have temp in the path under the directory C:\Windows.

DirectoryPathCSVs=C:\Windows DirectoryMustHaveCSVs=\*/temp/\* DirectoryCantHaveCSVs=

Include only the files that end with extension tmp or the directory name has xml in the path.

DirectoryPathCSVs=C:\Windows DirectoryMustHaveCSVs=\*/xml/\*, \*.tmp DirectoryCantHaveCSVs=

Include only the files that end with the extension txt under the UNIX directory

/home/data.

DirectoryPathCSVs=/home/data DirectoryMustHaveCSVs=\*.txt DirectoryCantHaveCSVs=

## Example configuration for scanning with exclude filters

Scan selected files and directories using the exclude filters.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

Exclude all the files with extension exe in the directory C:\Windows.

DirectoryPathCSVs=C:\Windows DirectoryMustHaveCSVs= DirectoryCantHaveCSVs=\*.exe

Exclude all files that end with extension tmp or if the directory name contains bin under the UNIX directory /home/data.

DirectoryPathCSVs=/home/data DirectoryMustHaveCSVs= DirectoryCantHaveCSVs=\*/bin/\*, \*.tmp

## Example configuration for scanning with include and exclude filters

Scan selected files and directories using both the include and exclude filters.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

Scan all directories with temp in the path or ending with pdf. Exclude files under the bin directory or ending with tmp under the directory C:\data.

DirectoryPathCSVs=C:\data DirectoryMustHaveCSVs=\*/temp/\*, \*.pdf DirectoryCantHaveCSVs=\*/bin/\*,\*.tmp

## Example configuration for scanning with date filtering

The parameters DirectoryBeforeDate and DirectoryAfterDate let you specify a date range within which documents must be modified for the scanner to process them.

Use the parameter DirectoryAfterDate to enter a number of days relative to the current date after which the page must be modified. A negative number specifies a date in the past.

User the parameter DirectoryBeforeDate to enter a number of days relative to the current date before which the page must be modified.

In the examples, both DirectoryBeforeDate and DirectoryAfterDate are required.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

Scan all the pdf files that have been modified in the last six months.

DirectoryMustHaveCSVs=\*.pdf DirectoryAfterDate=-180 DirectoryBeforeDate=0

Scan all files that have been modified between 60 days and 360 days in the past.

DirectoryAfterDate=-360 DirectoryBeforeDate=-60

## Example configuration for scanning with file size filtering

Scan files using file size filtering to limit what is scanned.

This configuration is in the file VontuFileSystemScanner.cfg.

See "Configuration options for file system scanners" on page 1321.

Scan all the files in the size range of 3000 bytes to 4000 bytes. Do not import any files that fall outside the size range.

ImportPreImportMinLength=3000 ImportPreImportMaxLength=4000 ImportEmptyFiles=false

Scan all doc files greater than 4 KB.

DirectoryMustHaveCSVs=\*.doc ImportPreImportMinLength=4096 ImportEmptyFiles=false

# **Example configuration for scanning that skips** symbolic links on UNIX systems

Scan a UNIX system, but skip all the symbolic links.

Specify a file which contains all the files that the scanner should scan. Only those files are scanned during the run. Place this file outside the scanner installation directory. In the example, this file is named /opt/test/filenames.txt.

This configuration is in the file <code>VontuFileSystemScanner.cfg</code>.

See "Configuration options for file system scanners" on page 1321.

Make sure that the DirectoryPathCSVs and related parameters are commented out. Also, make sure that the parameter PollingMethod is present only once in the configuration file.

PollingMethod=1 FilePollFilename=/opt/test/filenames.txt

# Setting up scanning of Web servers

This chapter includes the following topics:

- Setting up remote scanning of Web servers
- Supported Web server (scanner) targets
- Installing Web server scanners
- Starting Web server scans
- Configuration options for Web server scanners
- Example configuration for a Web site scan with no authentication
- Example configuration for a Web site scan with basic authentication
- Example configuration for a Web site scan with form-based authentication
- Example configuration for a Web site scan with NTLM
- Example of URL filtering for a Web site scan
- Example of date filtering for a Web site scan

# Setting up remote scanning of Web servers

The Web server scanner can retrieve Web site documents.

The Web server scanner uses crawlers to find Web pages and to process the Web pages for content and links to other Web sites. After a crawler has finished retrieving documents from the Web site, the Web server scanner imports the content that the crawler has retrieved into index file format (IDX). The scanner then posts the IDX

files to Network Discover for content processing. The Web server scanner can retrieve content from various document types, including Web documents, Word, Excel. and PDF files.

The Web server scanner crawls Web pages for links and content. The crawler processes the page content and either accepts or rejects the page for retrieval. If the page is accepted, the crawler looks for links from the page, filters the links and queues the accepted links for the crawler process. If the page is rejected, the crawler looks for links only if you have configured it to follow links on rejected pages. The links are filtered before they are added to the crawler queue. The crawler then retrieves the page content of accepted pages. The crawler requests the next link in its queue, and the process repeats.

To set up scanning of Web servers, complete the following process:

Table 66-1 Setting up a Web server scanner

Step	Action	Description
1	The Web server scanner can scan Web sites.  It has been tested with IIS and Apache Web servers.	See "Supported Web server (scanner) targets" on page 1328.
2	On the server with read access to the Web site, install the Web server scanner.	See "Installing Web server scanners" on page 1329.
3	Perform any manual configurations by editing the configuration files and properties files.	See "Configuration options for Web server scanners" on page 1332.
4	On the Enforce Server, add a new Scanner File System target.	See "Adding a new Network Discover target" on page 1187.
5	Start the file system scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See "Starting Web server scans" on page 1331.
6	Verify that the scan is running successfully.	See "Troubleshooting scanners" on page 1307.

## Supported Web server (scanner) targets

The Web server scanner supports scanning of a static HTTP Web site.

## **Installing Web server scanners**

The Web server scanner must be installed on the computer that has access to the Web sites that you want to scan.

#### To install the Web server scanner

On the computer with the file system to scan, download or copy (as binary) the relevant installation file to a temporary directory. The file is located in the DLP Home\Symantec DLP 12 Win\Scanners Of DLP Home/Symantec DLP 12 Lin/Scanners directory, where DLP Home is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

The file is one of the following file names:

- SymantecDLPScanners windows x32 12.5.exe
- SymantecDLPScanners Unix 12.5 x32.sh (for 32-bit Linux systems)
- 2 Start the scanner installation program.

Use the -c flag to install a scanner with a console command (rather than with a GUI).

#### Windows GUI:

```
SymantecDLPScanners windows x32 12.5.exe
```

#### Linux GUI:

./SymantecDLPScanners Unix x32 12.5.sh

#### Linux console:

```
./SymantecDLPScanners Unix 12.5.sh -c
```

- Confirm the version of the scanner you want to install (32-bit or 64-bit).
- 4 Confirm the license ageement.
- 5 Select Web Server Scanner.
- Select the installation **Destination Directory** (the directory where you want the Web server scanner installed).

Click Next.

Select the Start Menu Folder (shortcut in the Start menu). The default is Symantec DLP WebServer Scanner.

Click Next

- 8 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or host name of the Network Discover Server)
  - Discover Port

#### Click Next.

- Configure the Web server scanner by entering the following information:
  - Start URL

Enter the URL where the scan starts.

Include Filter

Only the paths that include all the strings specified here are scanned. Delimit entries with a comma, but do not use any spaces. Wildcards are supported.

Path Exclude Filter

Everything but the paths that contain the strings specified here are scanned. Delimit entries with a comma, but do not use any spaces. Wildcards are supported.

#### Click Next

- 10 The scanner installs.
- 11 Select the Startup Mode.

While you initially test or verify that the scanner runs successfully, do not select either of these options, but start the scanner manually.

You can select one (or none) of the following options:

- Install as a service on a Windows system.
- Start after installation.

#### Click Next

Click Finish.

- 12 The Web server scanner installation is complete on the scanner computer.
- 13 Perform any manual configurations by editing the configuration files and properties files.

See "Configuration options for Web server scanners" on page 1332.

See "Scanner installation directory structure" on page 1309.

See "Scanner configuration files" on page 1311.

- 14 On the Enforce Server, create a **New Target** for the scanner Web server type.
- **15** Start the scan on both the scanner computer and the Enforce Server.

See "Starting Web server scans" on page 1331.

## Starting Web server scans

Make sure that the scanner is installed and configured on the target computer, and a new target is added on the Enforce Server.

See "Installing Web server scanners" on page 1329.

Then, you can start the scan.

The procedures are different for each of the following scenarios:

- One scanner per target (first procedure).
- Multiple scanners for one target (second procedure).

#### To start a Web server scan with one scanner for one target

Log on to the Enforce Server.

Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- Select the scan target from the target list, then click the Start icon.
- On the scanner computer, start the Web server scanner.

Click Start > Vontu WebServer Scanner > Vontu WebServer Scanner Console.

The scanner starts the process of scanning data.

See "How Network Discover scanners work" on page 1306.

5 If the scan does not progress normally, you can troubleshoot it.

See "Troubleshooting scanners" on page 1307.

6 Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

#### To start a Web server scan with multiple scanners for one target

On each of the scanner computers, start the Web server scanner.

Click Start > Vontu WebServer Scanner > Vontu WebServer Scanner Console.

Make sure that each of the scanners has started, and has posted information. Check the outgoing folder on each of the computers.

See "Scanner installation directory structure" on page 1309.

Log on to the Enforce Server.

Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- 3 Select the scan target from the target list, then click the Start icon.
- 4 The scanner starts the process of scanning data.
  - See "How Network Discover scanners work" on page 1306.
- 5 If the scan does not progress normally, you can troubleshoot it. See "Troubleshooting scanners" on page 1307.
- Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

## **Configuration options for Web server scanners**

Table 66-2 provides an explanation of the VontuWebServerScanner.cfg file.

Parameters in the VontuWebServerScanner.cfg file **Table 66-2** 

Туре	Parameter	Description
Scanned Content	URL	A valid URL at which the crawler starts. If you want more than one page to be retrieved, the starting Web page must contain links to other Web pages. You must include the initial http:// in the configuration parameter.
Scanned Content	NavDirAllowCSVs	The list with include filters for paths. This list contains the strings that the URL of a page must contain for the scanner to process the page. Use the parameter NavDirCheck to specify how and when the scanner checks for these strings.  Use * for wildcard. Delimit entries with a comma, but do not use any spaces.
Scanned Content	NavDirDisallowCSVs	The list with exclude filters for paths. This list contains the strings that the URL of a page must not contain for the scanner to process the page. Use the parameter NavDirCheck to specify how and when the scanner checks for these strings.  Use * for wildcard. Delimit entries with a comma, but do not use any spaces.

Parameters in the VontuWebServerScanner.cfg file (continued) **Table 66-2** 

Туре	Parameter	Description
Scanned Content	NavDirCheck	A bitwise mask number that is used to determine where and how the scanner checks for the NavDirAllowCSVs strings and NavDirDisallowCSVs strings. If the URL of a page does not contain one of the NavDirAllowCSVs strings or does contain one of the NavDirAllowCSVs strings or does contain one of the NavDirDisallowCSVs strings, the scanner does not process the page.  See "Example of URL filtering for a Web site scan" on page 1336.
Scanned Content	Extensions	Enter file extensions to restrict the document types the scanner can crawler. To enter multiple extensions, separate them with commas . Use * for wildcard. No spaces before or after commas.  Example to only fetch the documents that have .doc or .html as extensions:  Extensions=*.doc, *.html*
Scanned Content	MaxLinksPerPage	The maximum number of links a page can have. Pages with many links are often navigation pages and this parameter can be used to filter them out.
Scanned Content	StayOnSite	You can configure the crawler to stay on the Web site on which it starts, or allow it to follow links to external Web sites in domains different from the starting Web site. By default, the crawler stays on the starting Web site domain.
Scanned Content	AfterDate	Number of days after which a page must be modified before it is saved. Enter the number of days relative to the current date. A negative number specifies a date in the past.
Scanned Content	BeforeDate	Number of days before which a page must be modified before it is saved. Enter the number of days relative to the current date. A negative number specifies a date in the past.

#### Parameters in the VontuWebServerScanner.cfg file (continued) **Table 66-2**

Туре	Parameter	Description
Authentication	LoginMethod	The authentication method for the site. The value must be AUTHENTICATE, FORMPOST, or FORMGET.
		See "Example configuration for a Web site scan with basic authentication" on page 1335.
		See "Example configuration for a Web site scan with form-based authentication" on page 1336.
Authentication	LoginURL	The page that contains the logon form.
Authentication	LoginUserValue	The user name to use for authentication (plain text or encrypted).
Authentication	LoginPassValue	The password to use for authentication. Encrypt this password.
		See "Encrypting passwords in configuration files" on page 1197.
Authentication	LoginUserField	The name of the user name form field (for FORMPOST or FORMGET logon methods).
Authentication	LoginPassField	The name of the password form field (for FORMPOST or FORMGET logon methods). Encrypt this password.
		See "Encrypting passwords in configuration files" on page 1197.
Proxies	ProxyHost	The host name or IP address of the proxy server.
Proxies	ProxyPort	The port number of the proxy server.
Proxies	ProxyUsername	The user name (plain text or encrypted) for the proxy server.
Proxies	ProxyPassword	The password for the proxy server. Encrypt this password.
		See "Encrypting passwords in configuration files" on page 1197.
Throttling	PageDelay	Number of seconds between downloading a page and requesting the next page.

Table 66-2 Parameters in the VontuWebServerScanner.cfg file (continued)

Туре	Parameter	Description
Throttling	BatchSize	The number of files that are aggregated into each XML file that is sent to Network Discover.

## Example configuration for a Web site scan with no authentication

Scan a Web site with no authentication.

This configuration is in the file VontuWebServerScanner.cfg.

See "Configuration options for Web server scanners" on page 1332.

```
URL=http://www.cnn.com
```

## Example configuration for a Web site scan with basic authentication

Scan a Web site that is protected with standard authentication.

This configuration is in the file VontuWebServerScanner.cfg.

See "Configuration options for Web server scanners" on page 1332.

```
Jobs
URL=http://site.domain.com
LoginURL=http://domain.server.com/login.html
LoginMethod=AUTHENTICATE
LoginUserValue=some user
LoginPassValue=9sfIy8vw
```

## Example configuration for a Web site scan with form-based authentication

Scan a Web site that is protected with form-based authentication.

This configuration is in the file VontuWebServerScanner.cfg.

See "Configuration options for Web server scanners" on page 1332.

```
//#
   Johs
URL= http://wiki.symantec.corp/dashboard.action
LoginMethod=FORMPOST
LoginURL=http://wiki.symantec.corp/login.action
LoginUserField=os username
LoginUserValue=some user
LoginPassField=os password
LoginPassValue=9sfIy8vw
```

## Example configuration for a Web site scan with NTLM

Scan a Web site that is protected with NTLM.

Make sure the NTLMUsername is in the format of Domain\user name.

This configuration is in the file <code>VontuWebServerScanner.cfg</code>.

See "Configuration options for Web server scanners" on page 1332.

```
Jobs
URL=http://some site
NTLMUsername=Some Domain\some domain user
NTLMPassword=9sfIy8vw
```

## Example of URL filtering for a Web site scan

Use the parameter NavDirCheck to determine where and how the scanner checks for the NavDirAllowCSVs strings and NavDirDisallowCSVs strings.

Create the NavDirCheck number by adding together some of the following numbers:

Parameter	Value	Description
URL	1	You must enter 1 to enable the scanner to check whether the URL of a page contains any of the strings that are specified in the parameter NavDirAllowCSVs or NavDirDisallowCSVs.
Case insensitive	64	If you add 64 to the URL value, the scanner checks the URL of a page for a match for the strings that are specified in the parameter ${\tt NavDirAllowCSVs}$ or ${\tt NavDirDisallowCSVs}$ . This match is not case-sensitive .
Before download	128	If you add 128 to the URL value, the scanner checks whether the URL has any NavDirAllowCSVs or NavDirDisallowCSVs strings before the page is downloaded.
Valid site structure	512	If you add 512 to the URL value, the scanner rechecks the <code>NavDirAllowCSVs</code> and <code>NavDirDisallowCSVs</code> values for the site to ensure that the site is still valid before it updates it. If you do not include this setting, then changes to these values are never checked. If the site is not valid, it is not downloaded.

In the following example, the scanner checks the URLs for matches for the strings "archive" or "test." This match is not case-sensitive, and part of a word or a whole word is matched. If the URL contains one of these strings, the page is not processed.

```
NavDirDisallowCSVs=*archive*, *test*
NavDirCheck=65
```

In the following example, the scanner checks the URLs for matches for the strings "news" or "home." This match is not case-sensitive, and part of a word or a whole word is matched. If the URL does not contain one of these strings, the page is not processed.

```
NavDirAllowCSVs=*news*, *home*
NavDirCheck=65
```

## Example of date filtering for a Web site scan

The following example retrieves the documents that were modified 365 days before the current date and 7 days after the current date.

AfterDate=-365 BeforeDate=7

# Setting up scanning of Documentum repositories

This chapter includes the following topics:

- Setting up remote scanning of Documentum repositories
- Supported Documentum (scanner) targets
- Installing Documentum scanners
- Starting Documentum scans
- Configuration options for Documentum scanners
- Example configuration for scanning all documents in a Documentum repository

## Setting up remote scanning of Documentum repositories

The Documentum scanner scans Documentum repositories.

To set up scanning of Documentum repositories, complete the following process:

**Table 67-1** Setting up a Documentum scanner

Step	Action	Description
1	Verify that your Documentum repository is on the list of supported targets.	See "Supported Documentum (scanner) targets" on page 1340.

Step	Action	Description
2	The Documentum scanner can be installed on any computer that has network connectivity to the computer that hosts the Documentum Document Broker.	See "Installing Documentum scanners" on page 1340.
3	Perform any manual configurations by editing the configuration files and properties files.	See "Configuration options for Documentum scanners" on page 1344.
4	On the Enforce Server, add a new Scanner Documentum target.	See "Adding a new Network Discover target" on page 1187.
5	Start the Documentum scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See "Starting Documentum scans" on page 1343.
6	Verify that the scan is running successfully.	See "Troubleshooting scanners" on page 1307.

**Table 67-1** Setting up a Documentum scanner (continued)

## **Supported Documentum (scanner) targets**

The Documentum scanner supports scanning a Documentum Content Server 5.3.x or 6.6.x repository.

## **Installing Documentum scanners**

The Documentum scanner can be installed on any computer that has network connectivity to the computer that hosts the Documentum Document Broker.

#### To install and deploy the Documentum scanner

- On the computer that has network connectivity to the computer that hosts the Documentum Document Broker, download the installation file. Download or copy (as binary) the SymantecDLPScanners windows x32 12.5.exe file to a temporary directory. The file is located in the DLP Home\Symantec DLP 12 Win\Scanners where DLP Home is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.
- 2 Start the scanner installation program on this computer.

```
SymantecDLPScanners windows x32 12.5.exe
```

Note: This scanner should only be installed on 32-bit Windows servers.

- 3 Confirm the version of the scanner you want to install (32-bit).
- 4 Confirm the license ageement.
- 5 Select Documentum Scanner.
- Select the installation Destination Directory, the folder where you want the Documentum Scanner to be installed.

The default is c:\Program Files\DocumentumScanner\.

Click Next.

7 Select the Start Menu Folder (shortcut in the **Start** menu).

The default is **SymantecDLP Documentum Scanner**.

Click Next.

- 8 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or host name of the Network Discover Server)
  - Discover Port
- Click Next

10 Enter the following Documentum configuration values for the scanner:

Doc Broker The name of the server where the repository for the DocBase is Host stored. Doc Base The name of the repository you want the Documentum scanner to retrieve. User Name Specify an account with full access rights to the Documentum files you want to scan. Password Password for the account. This password is plain text in the configuration file. WebTop Host The host name of the Web interface to the Documentum content repository. **WebTop Port** The port number for the Web interface.

- 11 Click Next.
- 12 The scanner installs.
- 13 Select the Startup Mode.

While you initially test or verify that the scanner runs successfully, do not select either of these options, but start the scanner manually.

You can select one (or none) of the following options:

- Install as a service on a Windows system.
- Start after installation.

The default is to start the scanner manually.

- 14 The Documentum scanner installation is complete on the scanner computer.
- 15 Perform any manual configurations by editing the configuration files and properties files.

See "Configuration options for Documentum scanners" on page 1344.

See "Scanner installation directory structure" on page 1309.

See "Scanner configuration files" on page 1311.

16 After installing the Documentum scanner, copy the dmc140.dll file from your Documentum installation bin directory, to the \DocumentumScanner\scanner folder in the scanner installation directory.

See "Scanner installation directory structure" on page 1309.

- 17 On the Enforce Server, create a New Target for the scanner Documentum type.
- **18** Start the scan on both the scanner computer and the Enforce Server.

See "Starting Documentum scans" on page 1343.

### Starting Documentum scans

Make sure that the scanner is installed and configured on the target computer, and a new target is added on the Enforce Server.

See "Installing Documentum scanners" on page 1340.

Then, you can start the scan.

The procedures are different for each of the following scenarios:

- One scanner per target (first procedure).
- Multiple scanners for one target (second procedure).

#### To start a Documentum scan with one scanner for one target

- Log on to the Enforce Server.
  - Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.
- 2 Select the scan target from the target list, then click the Start icon.
- On the scanner computer, start the Documentum scanner.
  - Click Start > Vontu Documentum Scanner > Vontu Documentum Scanner Console.
- The scanner starts the process of scanning data.
  - See "How Network Discover scanners work" on page 1306.
- 5 If the scan does not progress normally, you can troubleshoot it.
  - See "Troubleshooting scanners" on page 1307.
- 6 Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

#### To start a Documentum scan with multiple scanners for one target

On each of the scanner computers, start the Documentum scanner.

Click Start > Vontu Documentum Scanner > Vontu Documentum Scanner Console.

Make sure that each of the scanners has started, and has posted information. Check the outgoing folder on each of the computers.

See "Scanner installation directory structure" on page 1309.

2 Log on to the Enforce Server.

> Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- 3 Select the scan target from the target list, then click the Start icon.
- The scanner starts the process of scanning data.
  - See "How Network Discover scanners work" on page 1306.
- 5 If the scan does not progress normally, you can troubleshoot it.
  - See "Troubleshooting scanners" on page 1307.
- Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

### **Configuration options for Documentum scanners**

Table 67-2 provides an explanation of the VontuDocumentumScanner.cfg file.

**Table 67-2** Parameters in the VontuDocumentumScanner.cfg file

Parameter	Description
DocBase	The name of the repository you want Documentum to retrieve.
UserName	Specify an account with access rights to the Documentum files you want to scan.
Password	Password for the account that is specified in UserName. Encrypt this password.
	See "Encrypting passwords in configuration files" on page 1197.

Parameters in the VontuDocumentumScanner.cfg file (continued) **Table 67-2** 

Parameter	Description
ExtensionCSVs	List of file types to scan (Include Filter), for example:
	ExtensionCSVs=*.doc,*.htm,*.ppt,*.xls
	Delimit with a comma (no space).
ImportRefReplaceWithCSVs	Comma-separated list of one or two values that are used to construct the URL of the scanned documents.
	first_value,second_value
	If the Documentum interface client is a Windows desktop or desktop client, then the first-value is concatenated to the left of the <b>document-id</b> . The second string is concatenated to the right, for example:
	first_valuedocument_idsecond_value
	If the Documentum Webtop (Web-based) interface is your client interface, only one value is necessary; for example:
	<pre>ImportRefReplaceWithCSVs= http://documentum-server.mycompany.com:80 webtop/component/drl?objectId=</pre>
AfterDate	A maximum age for documents to be scanned. For example, if you set AfterDate to five days, only documents that are no more than five days old are scanned. AfterDate looks at the last modified date.
	You can enter one of the following values:
	N hours
	N days
	N weeks
	N months
	The Documentum scanner does not support automatic incremental scanning, but you can manually perform incremental scans, by setting the AfterDate and BeforeDate parameters.

Parameters in the VontuDocumentumScanner.cfg file (continued)

Parameter	Description
BeforeDate	A minimum age for documents to be scanned. For example, if you set AfterDate to five days, only documents that are no more than five days old are scanned. AfterDate looks at the last modified date.
	You can enter one of the following values:
	N hours
	N days
	N weeks
	N months
FolderCSVs	Specify the repository folders from which to fetch documents. All entries must begin with a slash but cannot consist of a slash alone. Leave the entry blank to specify all folders. Cabinets are treated as folders. For example:
	FolderCSVs=/support,/clients,/marketing,

Table 67-3 shows the host parameter in the dmcl.ini file.

[DOCBROKER PRIMARY] host = documentum-server.mycompany.com

During installation of the Symantec Data Loss Prevention scanner, the host parameter is set in the dmcl.ini file. If the Documentum Document Broker (server) later changes, this file must be edited to point to the new server.

**Table 67-3** dmcl.ini file

**Table 67-2** 

Parameter	Description
host	The computer that hosts the Documentum Document Broker (server).

## Example configuration for scanning all documents in a Documentum repository

Scan all documents in the repository.

The configuration is in the file VontuDocumentumScanner.cfg.

#### See "Configuration options for Documentum scanners" on page 1344.

```
[JOBS]
NUMBER=1
0=Job0
[Job0]
DocBase=Vontu 1
UserName=Administrator
Password=mypassword
ImportRefReplaceWithCSVs=
 http://documentum-server.mycompany.com:8080/webtop/
 component/drl?objectId=
LogFile = Job0.log
```

# Setting up scanning of Livelink repositories

This chapter includes the following topics:

- Setting up remote scanning of Livelink repositories
- Supported Livelink scanner targets
- Creating an ODBC data source for SQL Server
- Installing Livelink scanners
- Starting Livelink scans
- Configuration options for Livelink scanners
- Example configuration for scanning a Livelink database

## Setting up remote scanning of Livelink repositories

The Livelink scanner can scan a Livelink database.

To set up scanning of Livelink repositories, complete the following process:

**Table 68-1** Setting up a Livelink scanner

Step	Action	Description
1	Verify that your Livelink repository is on the list of supported targets.	See "Supported Livelink scanner targets" on page 1349.

Step	Action	Description
2	Create an ODBC data source for SQL Server. Install the Livelink scanner.	See "Creating an ODBC data source for SQL Server" on page 1349. See "Installing Livelink scanners" on page 1350.
3	Perform any manual configurations by editing the configuration files and properties files.	See "Configuration options for Livelink scanners" on page 1354.
4	On the Enforce Server, add a new Scanner Livelink target.	See "Adding a new Network Discover target" on page 1187.
5	Start the Livelink scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See "Starting Livelink scans" on page 1352.
6	Verify that the scan is running successfully.	See "Troubleshooting scanners" on page 1307.

**Table 68-1** Setting up a Livelink scanner (continued)

## **Supported Livelink scanner targets**

The Livelink scanner supports scanning of Livelink Server 9.x targets.

## Creating an ODBC data source for SQL Server

This procedure assumes that the Livelink database is an SQL Server database. If you have an Oracle Livelink database contact Symantec Data Loss Prevention support for specific instructions.

To create an ODBC data source for SQL Server

- 1 Go to Control Panel > Administrative Tools > Data Sources (ODBC).
- Click the **System DSN** tab.
- 3 Click Add.
- Select SQL Server.
- 5 Give it a name (for example, "Livelink"). This name is referenced in the VontuLiveLinkScanner.cfg file.
- Click Next

- Select With SQL Server authentication using a login ID and password entered by the user.
- 8 Check the option for Connect to SQL Server to obtain default settings for additional configuration options and enter the SQL Server credentials.
- 9 Click Next. Accept the defaults.
- 10 Click Next. Accept the defaults.
- 11 Click Finish.

## **Installing Livelink scanners**

Install the Livelink scanner on a computer that has access to the Livelink database.

#### To install a Livelink scanner

- 1 Create an ODBC data source for SQL Server. See "Creating an ODBC data source for SQL Server" on page 1349.
- 2 On the computer that has access to the Livelink database, download the installation file. Download or copy (as binary) the SymantecDLPScanners windows x32 12.5.exe file to a temporary directory. The file is located in the DLP Home\Symantec DLP 12 Win\Scanners where DLP Home is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.
- 3 Start the scanner installation program on this computer.

```
SymantecDLPScanners windows x32 12.5.exe
```

Note: This scanner should only be installed on 32-bit Windows servers.

- Confirm the version of the scanner you want to install (32-bit).
- 5 Confirm the license ageement.
- Select Livelink Scanner.
- Select the installation Destination Directory, the folder where you want the Livelink Scanner to be installed.

The default is c:\Program Files\LivelinkScanner\.

Click Next.

8 Select the Start Menu Folder (shortcut in the **Start** menu).

The default is SymantecDLP Livelink Scanner.

Click Next.

- Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or host name of the Network Discover Server)
  - Discover Port

Click Next.

**10** Enter the following Livelink configuration values for the scanner:

LiveLink Host The host name or IP address of the Livelink server.

LiveLink Port The HTTP port of the Livelink server.

LiveLink User Name The user name to use when you scan.

LiveLink Password The password to use when you scan.

Encrypt this password.

See "Encrypting passwords in configuration files" on page 1197.

LiveLink Connection

Name

The Livelink API connection name. This name is the dbconnection in the opentext.ini file on the Livelink

server.

LiveLink API Port This port should be 2099 unless it has been changed in the

opentext.ini file on the Livelink server. The default is

2099.

The name of the ODBC data source on the computer running ODBC DSN

the Livelink scanner.

SQL User Name User name to use to connect to the ODBC data source.

SQL Password Password to use to connect to the ODBC data source.

Encrypt this password.

See "Encrypting passwords in configuration files" on page 1197.

Click Next.

- 11 The scanner installs.
- 12 Select the Startup Mode.

While you initially test or verify that the scanner runs successfully, do not select either of these options, but start the scanner manually.

You can select one (or none) of the following options:

- Install as a service on a Windows system.
- Start after installation.

The default is to start the scanner manually.

- 13 The Livelink scanner installation is complete on the scanner computer.
- 14 Perform any manual configurations by editing the configuration files and properties files.

See "Configuration options for Livelink scanners" on page 1354.

See "Scanner installation directory structure" on page 1309.

See "Scanner configuration files" on page 1311.

15 Copy the following files from the Livelink installation to the \LivelinkScanner\scanner folder:

- LAPI ATTRIBUTES.dll
- LAPI BASE.dll
- LAPI DOCUMENTS.dll
- LAPI USERS.dll
- LLKERNEL.dll
- 16 Create an ODBC data source for the database instance that Livelink uses. This data source is referenced in the VontuLivelinkScanner.cfg file.

See "Creating an ODBC data source for SQL Server" on page 1349.

- 17 On the Enforce Server, create a New Target for the scanner Livelink type.
- 18 Start the scan on both the scanner computer and the Enforce Server.

See "Starting Livelink scans" on page 1352.

### Starting Livelink scans

Make sure that the scanner is installed and configured on the target computer, and a new target is added on the Enforce Server.

See "Installing Livelink scanners" on page 1350.

Then, you can start the scan.

The procedures are different for each of the following scenarios:

One scanner per target (first procedure).

Multiple scanners for one target (second procedure).

#### To start a Livelink scan with one scanner for one target

Log on to the Enforce Server.

Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- 2 Select the scan target from the target list, then click the Start icon.
- On the scanner computer, start the Livelink scanner.

Click Start > Vontu Livelink Scanner > Vontu Livelink Scanner Console.

4 The scanner starts the process of scanning data.

See "How Network Discover scanners work" on page 1306.

5 If the scan does not progress normally, you can troubleshoot it.

See "Troubleshooting scanners" on page 1307.

Stop and restart the scanner whenever you make changes to the configuration file. To stop the scanner, type the control-C character in the console window.

#### To start a Livelink scan with multiple scanners for one target

1 On each of the scanner computers, start the Livelink scanner.

Click Start > Vontu Livelink Scanner > Vontu Livelink Scanner Console.

Make sure that each of the scanners has started, and has posted information. Check the outgoing folder on each of the computers.

See "Scanner installation directory structure" on page 1309.

Log on to the Enforce Server.

Go to Manage > Discover Scanning > Discover Targets to navigate to the list of targets.

- Select the scan target from the target list, then click the Start icon.
- The scanner starts the process of scanning data.

See "How Network Discover scanners work" on page 1306.

5 If the scan does not progress normally, you can troubleshoot it.

See "Troubleshooting scanners" on page 1307.

Stop and restart the scanner whenever you make changes to the configuration 6 file. To stop the scanner, type the control-C character in the console window.

## **Configuration options for Livelink scanners**

Table 68-2 provides an explanation of the <code>VontuLiveLinkScanner.cfg</code> file.

Parameters in the VontuLiveLinkScanner.cfg file **Table 68-2** 

Туре	Parameter	Description
Connectivity	OpenTextServer	The host name or IP address of the Livelink server.
Connectivity	OpenTextPort	The HTTP port of the Livelink server.
Connectivity	OpenTextUsername	The user name to use when you scan.
Connectivity	OpenTextPassword	The password to use when you scan. Encrypt this password.
		See "Encrypting passwords in configuration files" on page 1197.
Connectivity	LLConnection	The Livelink API connection name. This parameter is the name of the dbconnection in the opentext.ini file on the Livelink server.
Connectivity	LLApiPort	This value should be 2099 unless it has been changed in the opentext.ini file on the Livelink server.
Connectivity	DSN	The name of the ODBC data source on the computer that runs the Livelink scanner.
Connectivity	SQLUserName	User name to use to connect to the ODBC data source.
Connectivity	SQLPassWord	Password to use to connect to the ODBC data source. Encrypt this password.
		See "Encrypting passwords in configuration files" on page 1197.
Throttling	BatchSize	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover.
		See "Optimizing resources with Network Discover scan throttling" on page 1204.

## **Example configuration for scanning a Livelink** database

Scan everything in the Livelink database.

The configuration is in the file VontuLiveLinkScanner.cfg.

See "Configuration options for Livelink scanners" on page 1354.

```
//#
    Jobs
[JOBS]
Number=1
0=Job0
[Job0]
OpenTextServer=mydatabase-livelink.test.lab
OpenTextPort=80
OpenTextUsername=Admin
OpenTextPassword=livelink
LLConnection=LivelinkDB
LLApiPort=2099
DSN=livelink
SQLUserName=11dbuser
SQLPassWord=livelink
```

# Setting up Web Services for custom scan targets

This chapter includes the following topics:

- Setting up Web Services for custom scan targets
- About setting up the Web Services Definition Language (WSDL)
- Example of a Web Services Java client
- Sample Java code for the Web Services example

## Setting up Web Services for custom scan targets

The Web Services target type enables customers to write custom scanners. These custom scanners send content and metadata to Network Discover as Simple Object Access Protocol (SOAP) requests. The Network Discover Server becomes a Web Service host.

See "About setting up the Web Services Definition Language (WSDL)" on page 1357.

An example of a Java SOAP client is available.

See "Example of a Web Services Java client" on page 1357.

To set up custom Web Services for Network Discover, complete the following process:

**Table 69-1** Setting up a custom scan target

Step	Action	Description
1	Add a Web Services target type.	See "Adding a new Network Discover target" on page 1187.

Step	Action	Description
2	Start the scan.	Select the scan target from the target list, then click the Start icon.  See "Managing Network Discover target scans" on page 1209.
3	Save and modify the WSDL, and a create a client (such as a Java client), or SOAP request.	See "About setting up the Web Services Definition Language (WSDL)" on page 1357.  An example Java client is available.  See "Example of a Web Services Java client" on page 1357.
4	Run the client, and verify the results.	See "Example of a Web Services Java client" on page 1357.

Table 69-1 Setting up a custom scan target (continued)

## **About setting up the Web Services Definition** Language (WSDL)

The concrete Web Service Definition Language (WSDL) can be downloaded from the following URL when a Web Services target is running. The following port is the default. Enter the location of your Network Discover Server and port number.

http://discover server:8090/?wsdl

See the online Help for a Web Services sample WSDL and for a Web Services sample SOAP request.

## Example of a Web Services Java client

The following procedure and code provide an example of Web Services. This example sends content and metadata of all the files in a folder to the Network Discover Server.

#### To create and run a Web Services Java client

Log into the Enforce Server and create a Network Discover Web Services target type.

See "Adding a new Network Discover target" on page 1187.

Use the default settings. Note the scanner port number; the default is 8090.

- 2 Start the scan.
- Browse to the following URL:

```
http://discover server:8090/?wsdl
```

Save the page as a WSDL file named DiscoverSOAPTarget.wsdl in a folder (for example sample folder).

Edit the URL to replace port number 8090 if the scanner port number is different in step 1.

- Install the Java Development Kit (JDK), if it is not available on your system. 4
- Set the Java home to the folder where you installed the JDK.

```
JAVA HOME=jdk install dir
```

6 Install Apache CXF, an open source service framework.

See http://cxf.apache.org/

7 Transform the WSDL to Java code.

```
apache-cxf-installdir\bin\wsdl2java
        -client sample folder\DiscoverSOAPTarget.wsdl
```

Java source files are automatically created under packages

com.vontu.discover and com.vontu.wsdl.discoversoaptarget.

8 Edit a file named DiscoverSOAPClient.java in the sample folder and insert the Java code. Place the new code at the beginning of this file. Change the constants as needed.

See "Sample Java code for the Web Services example" on page 1359.

**9** Compile the Java code with the following command:

```
javac DiscoverSOAPClient.java
```

10 Run the program using the following command:

```
java DiscoverSOAPClient
```

11 On the Enforce Server, verify that the expected number of items are reported for the Network Discover target that is created in step 1.

## Sample Java code for the Web Services example

Enter the following source code at the beginning of the file named

DiscoverSOAPClient.java.

See "Example of a Web Services Java client" on page 1357.

```
import javax.xml.datatype.DatatypeFactory;
import javax.xml.namespace.QName;
import java.io.ByteArrayOutputStream;
import java.io.File;
import java.io.FileInputStream;
import java.net.URL;
import java.util.Date;
import com.vontu.discover.ComponentContentType;
import com.vontu.discover.ComponentType;
import com.vontu.discover.DocumentType;
import com.vontu.discover.ProcessDocumentsType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetPortType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetService;
import com.sun.org.apache.xerces.internal.impl.dv.util.Base6
public class DiscoverSOAPClient
   private static final QName SERVICE NAME = new QName(
       "http://www.vontu.com/wsdl/DiscoverSOAPTarget.wsdl",
       "DiscoverSOAPTarget Service");
   private static final String OWNER = "DiscoverSOAPClient";
    private static final String BODY = "This is the body";
   private static final String TYPE = "Text";
   private static final String ENCODING = "base64";
    //Change this value according to your needs
   private static final String TEST FOLDER NAME = "c:\\temp\\data";
```

```
//Change this based on your discover host name and scanner port
private static final String WSDL PATH =
       "http://localhost:8090/?wsdl";
public static void main(String []args)
    try
    {
        URL wsdl = new URL(WSDL PATH);
        File folder = new File (TEST FOLDER NAME);
        DiscoverSOAPTargetService service =
           new DiscoverSOAPTargetService(wsdl, SERVICE NAME);
        DiscoverSOAPTargetPortType client = service.getDiscoverPort();
        for(File file : folder.listFiles())
            if(file.isDirectory())
                //only files in the test folder are sent to Discover
                continue;
            System.out.println(file);
            ProcessDocumentsType processDocumentsType =
               new ProcessDocumentsType();
            DocumentType documentType = new DocumentType();
            processDocumentsType.getDocument().add(documentType);
            documentType.setOwner(OWNER);
            documentType.setURI(file.toString());
            GregorianCalendar time = new GregorianCalendar();
            time.setTime(new Date(file.lastModified()));
            documentType.setLastModifiedDate(
                DatatypeFactory.newInstance().
                newXMLGregorianCalendar(time));
            documentType.setLastModifiedDate(
                DatatypeFactory.newInstance().
                newXMLGregorianCalendar(time));
            //create a component
            ComponentType body = new ComponentType();
            documentType.setComponent(body);
            body.setName(file.getName());
            //add body
            ComponentContentType bodyContent =
```

```
body.setComponentContent(bodyContent);
                bodyContent.setType(TYPE);
                bodyContent.setContent(BODY);
                ComponentType attachment = new ComponentType();
                body.getComponent().add(attachment);
                attachment.setName(file.getName());
                //add some content to the component
                ComponentContentType attachmentContent =
                    new ComponentContentType();
                attachment.setComponentContent(attachmentContent);
                attachmentContent.setType(ENCODING);
                ByteArrayOutputStream bytes =
                    new ByteArrayOutputStream();
                FileInputStream in = new FileInputStream(file);
                byte[] buf = new byte[1024];
                for(;;)
                    int len = in.read(buf);
                    if(len == -1)
                        break;
                    bytes.write(buf,0,len);
                attachmentContent.setContent(
                    Base64.encode(bytes.toByteArray()));
                //make the SOAP call
                client.processDocuments(processDocumentsType);
            }
        }catch(Exception e)
        {
        }
    }
}
```

new ComponentContentType();

Section

# Discovering and preventing data loss on endpoints

- Chapter 70. Overview of Symantec Data Loss Prevention for endpoints
- Chapter 71. Using Endpoint Prevent
- Chapter 72. Using Endpoint Discover
- Chapter 73. Working with agent configurations
- Chapter 74. Working with Agent Groups
- Chapter 75. Managing Symantec DLP Agents
- Chapter 76. Using application monitoring
- Chapter 77. Working with Endpoint FlexResponse
- Chapter 78. Using Endpoint tools

## Overview of Symantec Data Loss Prevention for endpoints

This chapter includes the following topics:

- About discovering and preventing data loss on endpoints
- About policies for endpoints

## About discovering and preventing data loss on endpoints

Endpoint Discover and Endpoint Prevent are deployed using Symantec Data Loss Prevention agents and Endpoint Servers.

See "About Endpoint Prevent" on page 54. See "About Endpoint Discover" on page 54.

Endpoint Prevent and Endpoint Discover both apply Data Loss Prevention policies to protect your sensitive or at-risk data. Sensitive or at-risk data can include credit card numbers or names, addresses, and identification numbers. You can configure both of these products to recognize and protect the files that contain sensitive data.

See "How Endpoint Prevent works" on page 1367.

Endpoint Prevent stops sensitive data from moving off endpoints and supported virtual desktops. For example, Endpoint Prevent stops a file that contains credit card numbers from being transferred to eSATA, USB, or FireWire connected media. Endpoint Prevent stops sensitive the files from being transferred to network shares.

Also, Endpoint Prevent monitors and prevents data from being transferred over applications.

Endpoint Discover examines the local fixed drives of an endpoint and locates every file that contains the information that matches a policy. Endpoint Discover scans the endpoints to find the information that you have defined as at risk or sensitive.

See "How Endpoint Discover works" on page 1383.

You can configure agent settings, group agents, set response rules, check agent health, and troubleshoot agents.

Table 70-1 **Endpoint features** 

Feature	Description	Additional information
Agent configuration	You can set detection types and detection locations. You can specify file filters and bandwidth limits. You set the agent configuration to best suite your implementation and data security requirements.	See "About agent configurations" on page 1405.
Agent groups	You use agent groups to send agent configurations to groups of agents.	See "About agent groups" on page 1443.
Agent health and management	You can review DLP Agent health and complete troubleshooting and management tasks.	See "About Symantec DLP Agent administration" on page 1457.
Application monitoring	You can configure this feature to monitor applications for CD/DVD burning, IM, email, or HTTP/S clients.	See "About monitoring applications" on page 1503.
FlexResponse	You can create response rules that automatically remediate incidents.	See "About Endpoint FlexResponse" on page 1512.
Endpoint tools	You use Endpoint tools to complete various maintenance tasks on the endpoint, like shutting down watchdog services, inspecting the agent database, and restarting Mac agents.	See "About Endpoint tools" on page 1523.

## About policies for endpoints

Symantec Data Loss Prevention uses a two-tiered detection architecture to analyze activity on endpoints. Detection occurs either directly on DLP Agents or on the Endpoint Servers as required. Endpoint Servers can perform all types of detection, such as Exact Data Matching (EDM), Indexed Document Matching (IDM), and Directory Group Matching (DGM). Agents can perform Described Content Matching (DCM) and Indexed Document Matching (IDM). Symantec Data Loss Prevention can detect locally on keywords, regular expressions, and data identifiers. It must send input content to the Endpoint Server to detect on exact data fingerprints or indexed document fingerprints.

Note: Agents running on Mac endpoints can perform DCM detection.

Two-tiered detection has implications for the kinds of detection rules and response rules you can combine in a policy and use on endpoints. It also has implications for the optimization of system usage and performance of Symantec Data Loss Prevention on endpoints. As you create the policies that apply to endpoints, the following guidelines are recommended.

Do not create a policy that combines a server-side detection rule with an Endpoint Prevent response rule. For example, do not combine an EDM or DGM rule with an Endpoint Block or Endpoint Notify response rule. If a server-side detection rule triggers an Endpoint Prevent response rule, Symantec Data Loss Prevention cannot execute the Endpoint Prevent response rule, and the system displays an error message.

See "Author policies to limit the potential effect of two-tier detection" on page 364.

When creating an endpoint policy that includes a server-side detection rule, combine that detection rule with an agent-side detection rule in one compound rule. This practice helps Symantec Data Loss Prevention perform detection on the endpoint without sending the content to the Endpoint Server. Symantec Data Loss Prevention saves network bandwidth and improves performance by performing detection on the endpoint.

For example, you can couple an EDM detection rule with a keyword detection rule in one compound rule. In a compound rule, all conditions must be met before Symantec Data Loss Prevention registers a match. Conversely, if one condition is not met, Symantec Data Loss Prevention determines there is no match without having to check the second condition. For example, to register a match the content must meet the first condition AND all other conditions in the same rule. When you set up the compound rule in this way, the DLP Agent checks the input content against the agent-side rule first. If there is no match, Symantec Data Loss Prevention does not need to send the content to the Endpoint Server. However, if you create

a compound rule that involves a DCM or an EDM policy, the content is still sent to the Endpoint Server.

Before you combine a server-side detection rule (for example, an EDM rule) with an All: Limit Incident Data Retention response rule that retains original files for endpoint incidents, consider the bandwidth implications of retaining original files. When it sends data to an Endpoint Server for analysis, the DLP Agent sends either text data or binary data according to policy requirements. Whenever possible, DLP Agents send text to cut down on bandwidth use. By default, Symantec Data Loss Prevention discards original files for endpoint incidents. If a response rule retains original files for endpoint incidents, DLP Agents must send binary data to the Endpoint Server. In this case, make sure that your network can handle the increased traffic between DLP Agents and Endpoint Servers without degrading performance.

Combine agent-side detection rules (for example, DCM) with an Endpoint Prevent response rule in the same policy. Symantec Data Loss Prevention can execute an Endpoint Prevent response rule only when a DLP Agent detection rule triggers the response.

Table 70-2 lists detection and response rules that cannot be combined.

Table 70-2 Incompatible detection rules and response rules

Do not combine these server-based detection rules	with these Endpoint Prevent response rules.
<ul> <li>Content Matches Exact Data (EDM)</li> <li>Sender/User Matches Directory (profiled DGM)</li> <li>Recipient Matches Directory (profiled DGM)</li> </ul>	<ul> <li>Endpoint: Block</li> <li>Endpoint: Notify</li> <li>Endpoint: User Cancel</li> </ul>

See "Workflow for implementing policies" on page 293.

## Chapter

## Using Endpoint Prevent

This chapter includes the following topics:

- How Endpoint Prevent works
- About Endpoint Prevent monitoring
- About policy creation for Endpoint Prevent
- How to implement Endpoint Prevent

### **How Endpoint Prevent works**

Endpoint Prevent policies detect and block confidential information moving from endpoints or virtual desktops in your organization. The Endpoint Server either pushes policies to Symantec DLP Agents or applies policies directly to files that are sent from the Symantec DLP Agents. Depending on the type of policy that you create, the policy is applied either by the Symantec DLP Agents directly or by the Endpoint Server. When Symantec DLP Agents or Endpoint Servers detect an activity that violates a policy rule, an incident is generated. You can review and remediate the incidents that display in the endpoint incident list.

**Note:** Policy groups that are assigned to an Endpoint Server apply equally to all connected agents.

Endpoint Prevent can detect violations at the endpoint in a variety of ways including:

- Application monitoring
- CD/DVD events
- Clipboard events
- eSATA events (writing to eSATA removable drives)

- Network events (HTTP/HTTPS, instant messaging, email, FTP)
- Network share events (copying sensitive files to or from a network share)
- Print/fax events
- USB events (flash cards, SD cards)

See "About Endpoint Prevent monitoring" on page 1368.

See "About the DLP Agent store" on page 1414.

See "Workflow for implementing policies" on page 293.

## **About Endpoint Prevent monitoring**

Endpoint Prevent can perform many different types of monitoring. The following table provides references to the types of monitoring you can select.

**Table 71-1 Endpoint Prevent Monitoring** 

Type of Monitoring	
About removable storage monitoring	
About endpoint network monitoring	
About CD/DVD monitoring	
About print/fax monitoring	
About network share monitoring	
About clipboard monitoring	
About application monitoring	
About virtual desktop support with Endpoint Prevent	

Endpoint Prevent monitors the activity on endpoints regardless if they are connected to an Endpoint Server. If an endpoint is disconnected from the network and cannot connect to an Endpoint Server, Endpoint Prevent continues to monitor the endpoint. All incidents are stored in the Agent Store until the endpoint is re-connected to the Endpoint Server. If the Agent Store exceeds the specified size limit, older files are ejected until the size limit is no longer exceeded. Endpoint Prevent does not stop monitoring the endpoint if the Agent Store exceeds the specified size limit.

See "About the DLP Agent store" on page 1414.

# About removable storage monitoring

Endpoint Prevent lets you block data transferring from your hard drive to a removable media device. Removable media includes the following devices:

- Compact flash card
- eSATA removable drives
- FireWire connected device
- SD card
- USB flash drive

When the Symantec DLP Agent detects that a incident has occurred, the data is not transferred. An incident is created and sent to the Endpoint Server. When a incident occurs, the Symantec DLP Agent displays a pop-up notification to the user that informs the user that the incident has occurred. The notification also requires a justification for the file transfer. This justification appears in the incident snapshot.

See "Setting report preferences" on page 1008.

For example, User 1 copies a Microsoft Word file that contains medical records from an endpoint to a USB flash drive. The Symantec DLP Agent blocks this file from being transferred to the flash drive. When the file is blocked, a pop-up notification appears on the user's screen, stating that the file transfer is in incident of a specific policy. The pop-up notification also contains a justification component that allows the users to justify moving the file to the flash drive. The justification that the user enters into the pop-up window is visible on the incident snapshot for this incident.

See "About Endpoint Prevent monitoring" on page 1368.

# About endpoint network monitoring

Endpoint Prevent lets you monitor or block various types of network events. These events include the following:

- HTTP/HTTPS
- Email/SMTP
- FTP
- IM

Endpoint Prevent lets you block network violations regardless of whether the endpoint is connected to the corporate network or not. For example, a user takes a laptop out of the office and accesses a wireless Internet connection in a coffee shop. The Symantec DLP Agent can still detect, remove, or block any file, text, or email from transferring over the unsecured network. Incidents that are generated when the endpoint is not connected to the Endpoint Server are stored in a temporary database. The incidents remain in the database until the connection is re-established. After the connection to the Endpoint Server is re-established, the incidents are sent to the Endpoint Server.

Symantec DLP Agents can monitor HTTP or HTTPS Web pages and applications. For example, it can monitor and prevent sensitive information from transferring through Microsoft Internet Explorer, Mozilla Firefox, or any other HTTP application. HTTPS monitoring lets you monitor or prevent any files from being transferred through an encrypted HTTPS site accessible through Internet Explorer or Firefox Web browsers. HTTP and HTTPS prevention also allow blocking of email messages and attachments from being transferred through Web email applications. Incidents include destination IP, URL, and message information.

Endpoint Prevent monitors the most common email applications, Microsoft Outlook, and Lotus Notes. It can monitor and prevent any information transferring from these applications regardless of the email protocol. Attachments as well as content in the subject, body, and footer of the message are analyzed. Incidents include information about the sender, recipient, and the email message.

FTP monitoring prevents files from transferring to an outside file repository over the FTP protocol. For example, a user attempts to send a file that violates a policy to a remote file repository using the FTP application Mozilla Filezilla. Endpoint Prevent prevents the file from transferring to the FTP location. An incident is created for the violation and appears in the Endpoint reporting section of the Enforce Server. The incident snapshot contains information about which users attempted to send the file through FTP. It displays the violating file as well as the IP address of the destination FTP server.

Instant messaging applications such as AIM, MSN, and Yahoo Messenger are monitored. IM monitoring analyzes outgoing messages both on an individual message basis as well as on a session basis. For example, if a user opens a chat session with another person through IM, Endpoint Prevent analyzes each message that the user sends for sensitive information. Each of these messages is analyzed individually. At the same time, Endpoint Prevent analyzes the entire conversation for the sensitive information that may not be apparent from the individual messages. IM messages and files can also be blocked. An IM incident contains information regarding sender, recipient, and the content of the session.

**Note:** Some network types do not match on the file name monitoring condition. These network events do not contain file names and so cannot match on this condition. The network monitoring types that cannot match the file name condition include HTTP/HTTPS, IM message body and text, and Outlook message body and text.

All incidents are reported under the Endpoint Prevent in the Reports section.

See "About Endpoint Prevent monitoring" on page 1368.

# About CD/DVD monitoring

CD/DVD monitoring is compatible with all major CD/DVD burning applications that run on Windows Server 2003, XP, Vista, and Windows 7 32- and 64-bit operating systems.

Endpoint CD/DVD monitoring is designed to monitor specific file types. Performance filters are available in the agent configuration section. Use them to specify the file types that Endpoint Prevent monitors. You can also control the effect of the monitoring on the CD/DVD burning application.

To enable CD/DVD protection, you must select the CD/DVD toggle in the Agent Monitoring tab of the Endpoint Server configuration page. You can also create a policy for the files that are copied to a CD/DVD burner. Create a Protocol or Endpoint Destination rule with the CD/DVD as the destination. You must specify the content criteria for the policy. Policies can be created using AND/OR Boolean conditions. Specify the content criteria only using the AND condition in the policy builder.

For example, you want to create a policy that prevents files with the keyword Farallon from being burned to a DVD. Your DVD burning application is Roxio 9. Create a blank policy with a protocol or a device type rule. Select the CD/DVD device type and also match a Content Matches Keyword rule. Enter Farallon as the keyword. Finish creating the rule with an Endpoint Block response rule. After you save the policy, the Symantec DLP Agent blocks any file that contains the keyword Farallon from being burned to a DVD.

By selecting the CD/DVD device type, you have specified that the policy affects only files burned to a CD/DVD. Endpoint hard drives and USB connected media are not affected. By combining the device type and keyword match rules, you quarantee that Symantec DLP Agents block only files with the specified keyword. The agents do not block all of the files that are sent to the CD/DVD application. If you create the CD/DVD block rule without the conjoined keyword rule, the policy blocks every file that is sent to the burning application. Or, it would block the files that contain the keyword at the endpoint hard drive and USB connected media as well.

Note: Depending on the CD/DVD burning application you use, a file that contains confidential information is blocked or redacted. The redacted file contains no sensitive data. If the redacted file is written to the disk, that specific CD or DVD cannot be reused.

Note: Small files of less than 64 bytes are not detected when read by CD/DVD monitoring. Files over 64 bytes in size are detected normally.

See "About policies for endpoints" on page 1365.

See "About Endpoint Prevent monitoring" on page 1368.

# About print/fax monitoring

Endpoint Prevent lets you monitor and prevent sensitive information from being either printed or faxed. In Microsoft Windows, the mechanism for printing and faxing information is identical; therefore, the Endpoint Prevent mechanism is also identical. Endpoint Prevent can monitor print jobs started from within an application or using the native **Print** utility in Windows Explorer.

Endpoint Prevent analyzes each page of a file as it is sent to the printer or the fax machine. This means that the initial pages of the file may be printed or faxed if a violation is found in the middle of the file. For example, a user sends a 10-page document to a printer. If Endpoint Prevent finds a violation on page three it stops the print job. Pages one and two print but pages three through ten do not. Endpoint Prevent sends an incident to the Endpoint Server containing file information and the matching text.

**Note:** Endpoint Prevent does not monitor the text in the cover page of a fax.

The incident snapshot contains information regarding which endpoint sent the violating file, the violating file, and the printer name and the printer type. The printer type is a locally connected printer, a shared printer, or a network printer, or the user selected the **Print to file** option.

See "Setting report preferences" on page 1008.

See "About Endpoint Prevent monitoring" on page 1368.

# About network share monitoring

Network share monitoring prevents users from moving sensitive files between a network share and an endpoint and from an endpoint to a network share. Any endpoint response rule is applicable to network share monitoring.

The Copy to Local Drive feature prevents users from moving sensitive data from a network drive to a local drive using Windows Explorer. For example, you have a local drive labeled c: drive and a remote network share labeled q: drive. You can create a policy that prevents users from moving sensitive data from the g: drive to the c: drive.

The Copy to Share feature prevents users from moving sensitive data from a local drive to a network share drive. You can create a policy that blocks sensitive data from being copied from the c: drive to the q: drive.

Endpoint Prevent prevents the sensitive data that transfers through Windows Explorer as well as through third-party applications, file browsers, and command line interfaces that use any of the following Windows network redirector services:

- LAN Manager (LanMan)
- Remote Desktop Protocol (RDP)
- Web Distributed Authoring and Versioning (WebDAV)

The Copy to Share feature monitors network shares like Windows shares, DFS, NAS, UNIX shares that are configured through Samba, Microsoft Remote Desktop shares, and WebDav shares that are accessed through a default WebDAV redirector.

This feature does not monitor types of network share access that do not use the RdpDr redirector services. These services include FTP transfers, third-party applications, save-as operations, command line utilities, or copy and paste applications. These other types of network file share access are monitored by using the Local Drive endpoint channel detection feature of Symantec Data Loss Prevention.

See "Configuring file filters" on page 1412.

See "About Endpoint Prevent monitoring" on page 1368.

# About clipboard monitoring

Endpoint Prevent stops users from copying and pasting sensitive data from one application to another by the Windows Clipboard. Endpoint Prevent does not prevent users from copying and pasting sensitive within the same application.

For example, if a user copies sensitive information from a Word document and pastes it in an IM message, Endpoint Prevent blocks the transfer. The blocking occurs because copy and paste functions use the Windows Clipboard. The user receives a pop-up notification that states the reason why the transfer was blocked. In the Endpoint Report, the incident snapshot contains an incident and the text of the information pasted into the email message. Incidents are created at the time of the cut or copy action, not at the paste action.

See "Setting report preferences" on page 1008.

See "About Endpoint Prevent monitoring" on page 1368.

# About application monitoring

Application monitoring, which is available on the System > Agents > Application Monitoring screen, lets you monitor third-party applications for IM, email, or HTTP/S clients. By default, Symantec Data Loss Prevention only monitors applications such as AIM, Microsoft Outlook, or Mozilla Firefox. Examples of third-party applications include Skype, Mozilla Thunderbird, or Google Chrome. You can add applications using the Application Monitoring page.

Additionally, you can configure global changes to default applications. You can set Symantec Data Loss Prevention to monitor blacklist or whitelist items, CD/DVD applications, applications that use Clipboard functions, and applications that upload content to the Internet.

See "About monitoring applications" on page 1503.

# About virtual desktop support with Endpoint Prevent

Endpoint Prevent can monitor virtual desktops and prevent remote users from copying sensitive data that is accessible through a virtual desktop. A Symantec DLP Agent can be installed in each virtual desktop. By running a DLP Agent in the virtual host, you can prevent a user from copying confidential data that is accessible from the hosted virtual desktop to a remote computer or device that may not be secure. You can configure Symantec DLP Agent to monitor storage volumes, print and fax requests, clipboards, and network activity on the virtual desktop.

Endpoint Prevent can monitor virtual desktops hosted by any of the following virtualization software:

- Microsoft Hyper-V virtualization server
- Microsoft Remote Desktop Services
- VMware View virtualization server

Endpoint Prevent can also be used to monitor virtual Windows desktops and Windows applications that are hosted through Citrix XenDesktop and Citrix XenApp/Application servers. Symantec supports deploying the Symantec DLP Agent software directly on Citrix XenApp/Application servers or Citrix XenDesktop virtual machines to prevent clients from extracting confidential data from Citrix published applications or desktops to the client computer. Symantec Data Loss Prevention provides this functionality by monitoring volumes, print/fax requests, clipboards, and network activity on the Citrix server to detect when confidential data would be sent to a client computer. A Symantec DLP Agent does not need to be installed on each individual Citrix client to support this functionality. A single Symantec DLP Agent monitors all of the Citrix clients. All Citrix clients that are

protected by the agent monitor need to have a valid Endpoint Prevent license. The license is required whether a Symantec DLP Agent is installed on the client or not.

Note: All incidents that are generated on Citrix drives by the Symantec DLP Agent software appear as Removable Storage Device incidents. In the Enforce Server administration console, you cannot deselect the Removable Storage event for Citrix drives because this event is always monitored by agents that are deployed to Citrix servers.

See "How Endpoint Prevent works" on page 1367.

# About policy creation for Endpoint Prevent

Endpoint Prevent policies execute DCM and VML conditions locally on the endpoint. An Endpoint Prevent policy contains a response rule that creates a real-time user interaction. The user interaction either blocks a file transfer or notifies the user of a policy violation. These notifications are then attached to the incident.

Endpoint policies also differ as to where the detection occurs. Detection for IDM, EDM, and DGM policies is performed on the Endpoint Server. Detection for DCM policies is performed directly by the Symantec DLP Agent.

The response rules Block, Notify, and User Cancel are performed only by the Symantec DLP Agent.

Because detection for IDM, EDM, and DGM policies is performed on the Endpoint Server, the detection takes more time and uses more bandwidth. Extra time and bandwidth are required because file contents are sent to the Endpoint Server for detection. When an agent performs detection for a DCM policy, it sends only incidents to the Endpoint Server.

See "About policies for endpoints" on page 1365.

See "Workflow for implementing policies" on page 293.

# About monitoring policies with response rules for Endpoint Servers

Endpoint-specific response rules include Endpoint Block, Endpoint Notify, Endpoint Quarantine, and User Cancel. Endpoint Block stops the movement of data that violate policies. Endpoint Notify educates the user about the violation that has occurred, but does not block or stop movement of the data. Endpoint Quarantine moves a file with sensitive information from the local drive to a secure location. Endpoint Quarantine is only applicable for Endpoint Discover. User Cancel lets the endpoint user decide whether or not to allow the data to transfer. All rules create a pop-up display window that contains information about the violated policy. Each

rule requests that the user provide a justification for the action. Endpoint Block and Endpoint Notify, and User Cancel are applicable to all Endpoint Prevent detection policies that are performed on the endpoint. For example, HTTP/HTTPS. Email/STMP, FTP, CD/DVD, eSATA, Print/Fax, and USB monitoring all use Endpoint Block or Endpoint Notify rules.

The Endpoint Notify and Block and User Cancel response rules are not applicable to:

- Violations that are found through Endpoint Discover
- Violations on local drive monitoring

See "Workflow for implementing policies" on page 293.

### **About Endpoint Block**

You can create a policy to restrict any data from transferring from the endpoint. For example, you want to stop any text, email, or file that contains the keyword Farallon from transferring from the computer. You can create a keyword match policy with the word Farallon as the violation keyword.

See "Workflow for implementing policies" on page 293.

You want to ensure that this policy is used across all endpoints. In the response rules section, select **Endpoint Block** as the response rule. This response rule is only applicable to the endpoint. If a file is transferred from the hard drive to a CD/DVD drive, a pop-up notification appears on that specific endpoint. The notification states that the action is in violation of the *Farallon* keyword policy.

The Endpoint Block response rule prevents the file from being moved. However, you also want to have a record of why the violation occurred. In the response rule, you can create a series of justifications. These justifications allow the endpoint user who committed the violation to explain why the violation occurred. These justifications can include user education, a manager-approved file move, or others.

## **About Endpoint Notify**

You can create a policy and a response rule that educates endpoint users by using the Endpoint Notify response rule. The Endpoint Notify response rule displays a pop-up message describing the violation and educates the endpoint user on the appropriate policy.

For example, an endpoint user sends an email that contains the word Farallon in the body of the email. Endpoint Notify generates an incident that is sent to the Endpoint Server and displays a pop-up notification on the endpoint. The notification states the policy that was violated and that the endpoint action is now monitored. The endpoint user enters a reason for the violation, accepts the notification, and

the email proceeds normally. Endpoint Notify does not prevent data movement, it only notifies users of policy violations. The endpoint user's justification for the violation becomes part of the incident report that is sent to the Enforce Server.

Not all policy groups and policies are applicable with Endpoint response rules. If you try to create a policy with incompatible rules and responses, you will receive an error message. The error states that the policy is incompatible with the Endpoint response rules.

Response rules can distinguish between those incidents that are created on the corporate network and those created off of the corporate network. This condition lets you specify whether the rule operates at all times or only when the endpoint is connected or disconnected from the corporate network.

### **About Endpoint User Cancel**

You can create a response rule that lets endpoint users decide whether or not to allow sensitive data to transfer from their computers. You can use the User Cancel response rule to educate your endpoint users on proper business policies. For example, if an endpoint user sends sensitive information through email and receives the User Cancel popup notification, they can cancel the data transfer. They are now educated on your company's policies. Additionally, if there is a legitimate need for the endpoint user to transfer sensitive data, they can allow the action. If they allow the action, the data is transferred normally.

In both cases, the Symantec DLP Agent generates an incident that is sent to the Enforce Server.

Endpoint users are only allowed a specific amount of time to decide whether or not to override the policy. If the specified amount of time is exceeded, the policy automatically blocks the data transfer and generates an incident. By default, the time is limited to 60 seconds. That option is applied to all violations of that policy that occur in the following 10 seconds.

If multiple violations of the same policy are blocked, the endpoint user must only enter the justification once. The justification appears in the incident snapshot of the incident. The incident snapshot also contains the action that was taken. The incident snapshot contains one of the following actions:

User Notified, Action: Allowed

User notified, Action: Canceled

User Notified, Action: Timeout Canceled

User Notified, Action: Timeout Allowed

Note: You can specify whether or not to allow the default action of a timeout to block the data transfer or allow it.

See "Configuring the Endpoint Prevent: User Cancel action" on page 928.

See "About policies for endpoints" on page 1365.

# How to implement Endpoint Prevent

Endpoint Prevent monitors each endpoint for the data that is moved from one place to another. If Endpoint Prevent detects a violation, it blocks the data from being transferred. Endpoint Prevent notifies the user of the violation and can require a justification from the user. Implementing Endpoint Prevent requires that you complete the following processes in order.

**Table 71-2** Implementation steps

Step	Action	For more information	
1	Add an Endpoint Server.	See "Adding a detection server" on page 194.	
2	Create endpoint agent configurations.	See "About agent configurations" on page 1405.	
3	Set the endpoint location. This is an optional step.	See "Setting the endpoint location" on page 1378.	
4	Install the Symantec DLP Agent.	For installation details, see the appropriate Symantec Data Loss Prevention Installation Guide.	
5	Create an endpoint policy.	See "About policy creation for Endpoint Prevent" on page 1375.	
6	Create endpoint response rules.	See "Response rules for endpoint detection" on page 877.	
7	Configure reports.	See "About Symantec Data Loss Prevention reports" on page 1006.	

See "Introducing synchronized Directory Group Matching (DGM)" on page 653.

# Setting the endpoint location

The endpoint location is used to define how Symantec Data Loss Prevention determines whether or not the endpoint is connected to the corporate network. You can specify if you want the Endpoint Server to automatically detect if the endpoint is on the corporate network. You can also enter domain names or IP addresses to use to manually determine if the endpoint is connected to the network.

Using the automatic method to determine endpoint location, Symantec Data Loss Prevention identifies the computer as on or off the corporate network based on the DLP Agent connection to the Endpoint Server.

The automatic endpoint location method is explained in the following list:

- On the corporate network:
  - If the DLP Agent is connected to the Endpoint Server, Symantec Data Loss Prevention identifies the agent as on the corporate network. The DLP Agent connection to the Endpoint Server is transient, which means that the agent disconnects from the Endpoint Server after a prescribed period of time. During the transient connection period, Symantec Data Loss Prevention considers the agent as on the corporate network.
- Off the corporate network:

This status means that the DLP Agent is disconnected from the Endpoint Server. The DLP agent may become disconnected ungracefully from the Endpoint Server. For example, an ungraceful disconnection occurs when the network interface that connects the agent to the Endpoint Server becomes disconnected. If the DLP Agent is disconnected ungracefully, Symantec Data Loss Prevention identifies the endpoint as off the corporate network.

See "About agent status" on page 1463.

Note: 12.0.x and earlier agents display connection status based on their constant connection to an Endpoint Server. If they become disconnected from the corporate network, Disconnected displays on the Summary Reports for 12.0.x and Earlier Agents screen. See "Using the Summary Reports for 12.0.x and Earlier Agents screen" on page 1473.

Using the manual method to determine endpoint location means that you must first input a range of domain names or IP addresses. Symantec Data Loss Prevention then uses this information to determine if the endpoint is connected to the corporate network. If a range of domain names is configured, the DLP Agent performs a reverse DNS lookup on the host IP address. It then matches the retrieved DNS host names with the configured domain names in the list. If a range of IP addresses is configured, the DLP Agent matches the host IP address against the list of configured IP addresses. Each individual host IP address must be on the corporate network for the endpoint to be considered connected to the corporate network.

Domain names must not contain wildcard characters and should be simple suffixes; for example, symantec.com.

IP addresses may contain wildcard characters in place of a single block. For example, 192.168.\*.\*.

See "About Endpoint Prevent monitoring" on page 1368.

#### To set the Endpoint Location setting

- Go to **System > Agents > Endpoint Location**. The current endpoint location settings are displayed. By default, the endpoint location determination is set to Automatic.
- 2 Click Configure.
- 3 Select an item to configure how the Enforce Server determines endpoint location.
  - Select Automatically to let the Endpoint Server determine whether an agent is on or off the corporate network.

Note: You must use automatic endpoint location to identify Mac endpoint locations. Manual endpoint location is not supported for DLP Agents running on Mac endpoints.

- Select Manually and enter a list of domain names or IP addresses in the correct field. Enter only one domain name or IP address per line.
- Click Save.

The changes take effect after the agent reconnects to the Endpoint Server.

See "How to implement Endpoint Prevent" on page 1378.

See "Endpoint Server—basic configuration" on page 191.

## About Endpoint Prevent response rules in different locales

You can create different endpoint response rule notifications that are specific to the locale of an endpoint. A locale refers to the system locale setting in the operating system of the endpoint.

For example, you create response rule notifications in English, French, or Japanese. If a user's locale is specified as Japanese, the Japanese-language version of the notification appears on the user's screen. If a different user with a French locale violates the same policy, the French-language version of the notification appears.

The Enforce Server lets you specify multiple user notifications. However, the first language that is specified is the default language. You cannot delete the default language response notification. You can add or delete any notification or language that is not specified as the default language. At installation, the default language is set to whichever language is set as the Enforce Server language. If the language you want is unsupported, the Enforce Server tries to display the English-language notification.

For example, you have a Japanese-locale endpoint and a Vietnamese-locale endpoint. The Vietnamese locale is not a supported locale. If a violation occurs on the Japanese-locale computer, the Enforce Server displays the Japanese notification. If no Japanese notification is available, the Enforce Server displays the default-language notification. If the Vietnamese-locale computer violates a policy, the Enforce Server displays the English notification because no Vietnamese notification is possible. If the English notification is unavailable, the Enforce Server displays the default-language notification.

If the first language you add is not supported on the endpoint, that language cannot be considered the default language. The endpoint must contain the specific language details to consider a language as the default language. Although the text of the notification appears in the unsupported language, the notification window buttons and title bar appear in the default locale of the Enforce Server.

If you want to define an unsupported language as the default language, you must select **Other** as the first language. This **Other** label removes all other languages in the list. Use the Endpoint configuration options to modify the text of the pop-up window labels. You cannot specify other language responses if you select the Other option. The **Other** setting displays that language notification on every endpoint, regardless of the system locale of the endpoints.

See "Advanced agent settings" on page 1414.

Note: All English locales default to the English (United States) setting. All French locales default to the French setting. For example, the French (France) setting supports all types of French such as French (Canada) and French (France).

See "Setting Endpoint Prevent response rules for different locales" on page 1381.

## **Setting Endpoint Prevent response rules for different locales**

You can set different response rules for different locales. The first locale that you designate becomes your default locale. You cannot delete this locale, although you can delete additional locals.

See "About Endpoint Prevent response rules in different locales" on page 1380.

#### Setting a localized response rule

- 1 Go to Manage > Policies > Response Rules.
  - See "Configuring response rules" on page 891.
- 2 Create the response rule normally.
- 3 Click the **Add Language** link.
- 4 Select the language that you want to use.
  - If you want to specify an unsupported language as the default language, select Other.
- Enter text in the display fields and the justification fields using the designated 5 language.
- 6 Click Save.

# Chapter

# Using Endpoint Discover

This chapter includes the following topics:

- How Endpoint Discover works
- About Endpoint Discover scanning
- Preparing to set up Endpoint Discover
- Setting up and configuring Endpoint Discover
- Creating an Endpoint Discover scan
- Managing Endpoint Discover target scans

# **How Endpoint Discover works**

Endpoint Discover lets you examine a local drive in your organization for any data that is a potential risk. Endpoint Discover notifies you when it finds a file that violates your policies and it identifies where the file is located on the endpoint system. Endpoint Discover can scan any local drive that is connected to the endpoint. It cannot scan CD/DVD drives or removable media devices such as eSATA drives, USB flash drives, or SD cards.

See "About Endpoint Discover scanning" on page 1383.

# **About Endpoint Discover scanning**

Endpoint Discover scans the local drive of endpoints to find any currently existing files that violate your policies. Endpoint Discover scans all local drives on your endpoints. For example, if your computer has two physical local drives installed, Endpoint Discover scans both local drives for any files that violate your policies. Endpoint Discover does not scan those drives that are mounted through a network or removable media such as eSATA drives, flash drives, or SD cards.

The DLP Agent can only perform DCM scans locally for Endpoint Discover. For all other types of scans, the DLP Agent sends the text of the files to the Endpoint Server for analysis. Because the agent sends the files to the Endpoint Server. EDM detection must be done on the Endpoint Server, along with IDM if two-tier detection is enabled. See "Two-tier detection for DLP Agents" on page 309.

For example, you set up an Endpoint Discover scan to examine all of the local drives of all of your endpoints. The policy that is associated with the scan contains a DCM keyword condition as well as an EDM condition configured to match on credit card numbers. During the Endpoint Discover scan, the system automatically analyzes each file on the local drive for the keywords. If a policy matches a keyword, the content is sent to the Endpoint Server for EDM analysis.

To start or stop a scan that is configured for a single Endpoint Server, the DLP Agent must be connected to the Endpoint Server. If the DLP Agent is not connected to the Endpoint Server, the scan starts when it reconnects to the Endpoint Server. A scan is only complete when all of the endpoints have completed the scan. If one endpoint is disconnected from the Endpoint Server, the scan cannot complete until that endpoint reconnects or the scan times out. If an endpoint is disconnected after a scan has started, the endpoint continues the scan after it reconnects to the Endpoint Server. If the endpoint remains disconnected and exceeds a configured timeout period, the scan reports a timeout status.

An Endpoint Discover scan can be configured to include multiple Endpoint Servers. This feature lets you create one Endpoint Discover scan that includes a primary Endpoint Server and any backup Endpoint Servers that might be configured. Scans that include backup Endpoint Servers allow DLP Agents to be scanned if they connect to a backup Endpoint Server during an active scan. The ability to scan a DLP Agent when it connects to a backup Endpoint Server improves the ability of a scan to successfully complete. It also improves the performance of Endpoint Discover in a load-balanced environment.

All incidents are stored in the Agent Store until the computer is reconnected to the Endpoint Server. If the Agent Store exceeds the specified size limit, the scan waits until the Agent Store size is reduced. The scan waits until the endpoint reconnects to the Endpoint Server and the Agent Store is cleared.

See "About the DLP Agent store" on page 1414.

By default, the DLP Agent scans most of the files on the endpoint while the computer is active. Any file that requires a large amount of bandwidth to scan is not scanned until the endpoint is idle. By waiting until the endpoint is idle, the DLP Agent uses less CPU bandwidth while users are active on the computer. You can configure how the DLP Agent defines the endpoint as idle. You can configure the DLP Agent so that it does not scan the endpoint at all while the computer is active.

Note: DLP Agents running on Mac endpoints do not use CPU bandwidth management.

See "Advanced agent settings" on page 1414.

# About targeted Endpoint Discover scans

You can use targeted Endpoint Discover scans to do the following:

- Define an Endpoint Discover scan that uses multiple Endpoint Servers to target endpoints.
- Define an Endpoint Discover scan that targets individual endpoints.
- Define an Endpoint Discover scan that uses filters to scan groups of endpoints, specific locations on endpoints, files of a specific size, and so on. When the Endpoint Server begins the scan, the scan information is distributed to all of the associated DLP Agents. The DLP Agents analyze the scan with the scan filters.

Note: You cannot create Endpoint Discover scans that target Mac endpoints. However, you can create exclusion filters to scan specific files and locations on Mac endpoints. See "Using filters to scan Windows and Mac operating systems" on page 1399.

If a DLP Agent is excluded from the scan it sends a "Not participating" status to the Endpoint Server.

There can be only one Endpoint Discover scan running on an Endpoint Server at a time. If you exclude DLP Agents based on the scan filters, those DLP Agents cannot be scanned until the first scan is complete.

See "Creating an Endpoint Discover scan" on page 1389.

# Preparing to set up Endpoint Discover

Before you begin setting up and configuring Endpoint Discover scans, you must complete prerequisite steps.

Table 72-1 lists the steps you must complete.

Step	Action	More information
1	Add an Endpoint Prevent Server if one is not already present or modify an existing one.	An Endpoint Prevent Server provides monitor, prevent, and scanning features for DLP Agents.
		See "Endpoint Server—basic configuration" on page 191.
2	Create a policy group.	See "Creating a policy group for Endpoint Discover" on page 1386.
3	Create a policy.	See "Creating a policy for Endpoint Discover" on page 1387.
4	Add a rule.	See "Adding a rule for Endpoint Discover" on page 1387.

Table 72-1 Endpoint Discover prerequisite steps

See "Setting up and configuring Endpoint Discover" on page 1389.

# Creating a policy group for Endpoint Discover

Creating a policy group for Endpoint Discover is exactly like creating a policy group for Network Discover. Instead of deploying these policy groups on different nodes in your system, the policy groups are deployed through the Symantec DLP Agents. After you have created the policy group, you can assign specific policies to the policy group.

#### To create a policy group

- Go to Administration > Settings > Policy Groups. 1
- 2 On the **Policy Group List** screen that appears, click **Add Policy Group**.
- Enter a policy-group name (of up to 256 characters) and a description. Choose an informative name because other users must access it when choosing which policy group(s) to associate with roles, policies, and Endpoint Discover targets.
- Choose the detection server to assign to this policy group. This is an optional step.

You can assign the policy group to all detection servers or to individual servers. Note that Symantec Data Loss Prevention automatically assigns all policy groups to all Endpoint Discover servers.

5 Click Save.

See "Setting up and configuring Endpoint Discover" on page 1389.

# Creating a policy for Endpoint Discover

Symantec Data Loss Prevention uses two-tiered detection methods for Endpoint detection. Detection for Endpoint Discover occurs on the Endpoint Server and on the agent. The DLP Agent sends files to the Endpoint Server for analysis when two-tier detection is enabled. EDM and DGM policies are all performed on the Endpoint Server. The DLP Agent sends the opened files from the endpoint to the Endpoint Server for analysis.

See "About policies for endpoints" on page 1365.

You can set the status of the policy as either Active or Suspend. By default, policies are set to Active status. If you select Suspend, the policy is not applied to the DLP Agents.

The following instructions apply to creating a blank policy. You can also create policies based on pre-existing templates. The following instructions use sample data and specific instructions to illustrate how to create a policy.

#### To create a policy for Endpoint Discover

- 1 Go to Manage Policies > Policy List on the Enforce Server.
- 2 Click **Add Policy**, and click **Next**.
- 3 Select Add a blank policy.
- Enter a name to identity the policy in the **Name** field.
- 5 Enter details about the policy in the **Description** field of the new policy.
- Select the policy group you want associated with this policy from the drop-down menu.

After you create the policy, you must add rules to the policy.

See "Adding a rule for Endpoint Discover" on page 1387.

See "Setting up and configuring Endpoint Discover" on page 1389.

# Adding a rule for Endpoint Discover

After you have created a policy for Endpoint Discover, you must add rules to the policy. You can add one or more rules to the policy. You must add at least one rule to the policy.

See "Creating a policy for Endpoint Discover" on page 1387.

#### To add a rule to a policy

- Under the Detection tab, click **Add Rule** to add a rule for the policy.
- 2 Select the **Content Matches Exact Data from** radio option.

- 3 Select the policy you want to use in the drop-down menu. This procedure links the previously created list to the rule.
- Click Next.

See "Setting up and configuring Endpoint Discover" on page 1389.

#### **About Endpoint Quarantine**

You can create an automated response rule that allows Endpoint Discover to remove files from a local drive and place them in a secure location. If an Endpoint Discover scan finds a file containing sensitive data, the file is quarantined and removed from the non-secure location. The secure location can be either on the local drive or it can be a secure location on the corporate network. You can create marker files that replace the confidential data. The marker files alert endpoint users that the file contained confidential information and was guarantined. You can include variables in the marker text that describe aspects of the incident such as the file name, the violated policy, and the location of the secure folder.

Note: Endpoint quarantine is not available for DLP Agents running on Mac endpoints.

Endpoint quarantine response rules are only applicable to Endpoint Discover running scans on Windows endpoints.

The quarantine location can be either a secured folder on the local drive or a folder on a remote file share that is accessible by the endpoint through the corporate network. You can choose if you want to enable credentials on the secure location or allow any anonymous user to access the location.

Note: Encrypting File Service (EFS) folders cannot support anonymous access.

Not all policy groups and policies are applicable with Endpoint response rules. If you try to create a policy with incompatible rules and responses, you receive an error message. The error states that the policy is incompatible with the Endpoint response rules.

See "About policies for endpoints" on page 1365.

See "How to implement Endpoint Prevent" on page 1378.

See "Configuring the Endpoint Discover: Quarantine File action" on page 920.

# Setting up and configuring Endpoint Discover

To implement Endpoint Discover, you must follow a specific set of tasks. These tasks are similar to Network Discover, but not identical.

Complete the following configuration tasks:

Table 72-2 Implementing Endpoint Discover

Step	Action	More information
Step 1	Create an Endpoint Discover target.	See "Creating an Endpoint Discover scan" on page 1389.
Step 2	Install the Symantec DLP Agent.	For installation details, see the appropriate Symantec Data Loss Prevention Installation Guide.
Step 3	Configure reports.	See "About Symantec Data Loss Prevention reports" on page 1006.

See "Preparing to set up Endpoint Discover" on page 1385.

# Creating an Endpoint Discover scan

To create an Endpoint Discover scan, you set up an Endpoint Discover target. Later you configure the target meet your scanning requirements. When you configure scan settings you can set the scan to use multiple Endpoint Servers. You also configure Endpoint Discover targets to scan specific endpoints.

The Endpoint Discover target can also be configured to scan specific locations on endpoints. The scan can use filters to target local drives, folders, or endpoints to find policy violations. This filtering is called Targeted Endpoint Discover scanning. For example, the fixed drive or the My Documents folder in Windows can be configured as a target. Endpoint Discover can scan any fixed drive that is associated with the endpoint. Endpoint Discover cannot scan removable drives. You can also specify filters to determine which endpoints you monitor. Any endpoints that the Targeted Endpoint Discover scan excludes display as Not Participating.

**Table 72-3** Steps to configure scan settings for an Endpoint Discover scan target

Step	Description	More information
1	Configure a new Endpoint Discover target by clicking Manage > Discover Scanning > Discover Targets to	See "Creating a new Endpoint Discover target" on page 1390.

Step Description More information 2 Add location, date, and file type filters to the See "About Endpoint Discover Endpoint Discover target. You enter this target filters" on page 1392. information on the Filter tab on the Manage > Discover Scanning > Discover Targets screen. 3 Configure the scan idle timeout and max scan See "Configuring Endpoint duration settings. You set this information on the Discover scan timeout Advanced tab on the Manage > Discover settings" on page 1400. Scanning > Discover Targets screen .

**Table 72-3** Steps to configure scan settings for an Endpoint Discover scan target (continued)

Note: You cannot schedule Endpoint Discover targeted scans. Each scan must be started manually. You must also manually stop the scan, allow it to complete, or allow it to timeout. You cannot pause an Endpoint Discover scan.

# Creating a new Endpoint Discover target

For a new Endpoint Discover target, enter the name of the target, the policy group, and the Endpoint Server where the scans can run.

These required fields should be set when a new target is added.

#### To enter the required fields for a target

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- 2 Click New Target, and select File System under Endpoint.

3 Complete the following items on the **General** tab.

Name Enter a name for this Endpoint Discover target.

**Policy Group** Select the Endpoint Discover policy group you created.

See "Creating a policy group for Endpoint Discover" on page 1386.

If no other policy group has been selected, the Default Policy group is used. You can assign multiple policy groups to a target.

The administrator defines policy groups on the Policy Group List page. If the policy group you want to use does not appear on the list, contact your Symantec Data Loss Prevention administrator.

Servers Select the Endpoint Server (or multiple Endpoint Servers) where

you want to allow the scan to run.

Only the detection servers that were configured as Endpoint Servers appear on the list. You should configure your Endpoint Servers before you configure targets. You must specify at least one server before you can run a scan for this target.

See "Selecting multiple servers for an Endpoint Discover scan" on page 1392.

Configure items on the **Filters** tab.

You can configure the following:

- Add filters to specify items to include or exclude from a scan. See "About Endpoint Discover target filters" on page 1392.
- Specify maximum or minimum file sizes to scan. See "Filtering Discover targets by item size" on page 1201.
- Enable incremental and differential scan features. See "Scanning new or modified items with incremental scans" on page 1224. See "Scanning new or modified items with differential scans" on page 1225.
- Specify files to scan base on their last accessed or modified date. See "Filtering Discover targets by date last accessed or modified" on page 1202.
- 5 Configure settings on the Advanced tab.
- See "Configuring Endpoint Discover scan timeout settings" on page 1400. 6
- Click Save to save all updates to the target. 7

### Selecting multiple servers for an Endpoint Discover scan

You can add more than one Endpoint Server to an Endpoint Discover scan. Adding multiple servers helps improve scan performance.

If a DLP Agent loses its connection to the primary Endpoint Server during an Endpoint Discover scan, the agent can continue the scan by establishing a connection to a backup Endpoint Server using a failover or load balancer scenario. A user adds all failover Endpoint Servers installed behind a load balancer when creating or editing the Endpoint Discover scan target.

Connecting to additional servers also improves Endpoint Discover scan performance in load-balanced environments.

Note: Each time there are policy changes, the Enforce Server sends data to all Endpoint Servers associated with the Endpoint Discover scan, which potentially creates bandwidth issues.

# About Endpoint Discover target filters

Endpoint Discover target filters affect how Endpoint Discover interacts with your endpoints. Endpoint Discover target filters let you specify the following:

- The type of files you want to scan.
- The areas within the target you want to scan.
- The subset of endpoints you want to scan.
- The size of the files you want to scan.

Endpoint Discover targets are dedicated to a specific local system. Unlike Network Discover, endpoint targets do not need defined root systems or network shares.

See "Creating an Endpoint Discover scan" on page 1389.

See "Using include and exclude filters" on page 1392.

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

## Using include and exclude filters

Exclude and include filters let you reduce the number of items or repositories to scan.

Note: You cannot use exclude and include filters to target specific Mac endpoints. See "Using filters to scan Windows and Mac operating systems" on page 1399.

Use the **Include Filters** field to specify the items that Symantec Data Loss Prevention should process. If you leave the Include Filters field empty, Symantec Data Loss Prevention performs matching on all items in the selected target. If you enter any values in the field, Symantec Data Loss Prevention scans only those items that match your filter.

Use the **Exclude Filters** field to specify the items that Symantec Data Loss Prevention should not process. If you leave the **Exclude Filters** field empty, Symantec Data Loss Prevention performs matching on all items in the selected target. If you enter any values in the field, Symantec Data Loss Prevention scans only those items that do not match your filter.

Table 72-4 lists the items you can include or exclude by using filters.

Items that can be filtered **Table 72-4** 

Item to filter	Description	
Files	You can enter file extensions in the <b>Include Filters</b> and <b>Exclude Filters</b> to include or exclude file types, respectively.	
File folders	You can enter folder names in the <b>Include Filters</b> and <b>Exclude Filters</b> to include or exclude folders, respectively.	
IP addresses	Endpoint Discover uses a common syntax to describe IP address ranges. This format is similar to the standard Classless Inter-Domain Routing (CIDR) format. The Endpoint Discover IP address range filter format includes a main network address, a following "/" character, and the number of mask bits. For example, the IP address range description 192.64.110.0/24 has a mask bit count of 24. This means that all IP addresses from 192.64.110.0 – 192.64.110.255 match the filter. Likewise, 128.0.0.0/8 represents the IP address range 128.0.0.0 – 128.255.255.255.	
Computer names	You can enter the host name, FQDN name, or NetBIOS name. You can use the wildcard (*) character.	
WINS names	You can enter a WINS name to include or exclude endpoints.	

Table 72-5 table lists the syntax you can use when you add filters.

Syntax for the include filters and exclude filters Table 72-5

Syntax	Description
* (asterisk)	Use this wildcard to match zero or more characters.
	A *.* pattern added at the end of the path has the same behavior as a *. For instance a filter like C:\ep_test\data\edar* or C:\ep_test\data\edar*.* have the same meaning.
	If *.* separates a directory path, then Symantec Data Loss Prevention expects a file or folder with a period (.) that matches the pattern. For example, C:\ep_test\da*.*ta\edar would match c:\ep_test\da.ta\edar or c:\ep_test\da123.ta\edar, but it does not match c:\ep_test\data\edar.
	The *.txt,*.doc pattern of an include filter matches only files or documents with the .txt or .doc extensions and ignores everything else.
	A *.? pattern of an include filter only matches files or documents with a single-character extension. This example matches files such as hello.1 and hello.2, but not hello.doc or hello.html.
	A */documentation/*,*/specs/* pattern filters to match on specific subdirectories of a file share. This example filter pattern only matches the files that are contained in the two subdirectories that are called documentation and specs.
? (question mark)	Use this wildcard to match one character in the place where it appears.
, (comma)	Represents a logical OR. Delimit entries with a comma.
The forward slash (/) and backslash (\) These characters are equivalent. They usually represent separators, although on Linux and Mac the backslash is character in a file name.	
Escape characters	The matching process does not support escape characters, so there is no way to match a question mark, a comma, or an asterisk explicitly. In general, special characters in filter items are not supported.

Endpoint Discover does not include the following items in a scan:

- Mounted drives on Windows such as USB drives
- Windows network shares

See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

#### Setting up Endpoint Discover filters to include or exclude items from the scan

You use include and exclude filters to include or exclude files and locations from an Endpoint Discover scan.

#### To set up include filters or exclude filters:

- In the Enforce Server administration console, go to Manage > Discover Scanning > Discover Targets.
- Click the name of the scan where you want to add include filters or exclude filters.
- 3 Click the **Filters** tab.

By default, the **Exclude** field displays the following filters:

```
$Windows$/*,/Applications/*,/System/*,/.Spotlight*,*.mp3,*.wma,*.wav,
*.vox, *.aac, *.3qp, *.dat, *.avi, *.mpeq, *.wmv, *.mov, *.mp4, *.dylib, *.jar, *.dll, *.exe,
$ProgramFiles$/*,/opt/*,/sbin/*,/bin/*,/usr/bin/*
```

Enter file names or paths in the Include Filters field and the Exclude Filters field to select a subset of items that Symantec Data Loss Prevention should process. Delimit entries with a comma, but no spaces. The path filter is case-sensitive.

Use \* (asterisk) at the end of a path to include or exclude all content in the specified folder. For example, if you enter C: /Users/\*, /Users/\* in the Include Filter field, all contents in the C:Users folder on Windows endpoints and the /Users/ folder on Mac endpoints are scanned.

When both include filters and exclude filters are present, exclude filters take precedence.

The include filter and exclude filter file names are relative to the file system root. Specify full paths or subdirectories, as needed. Some wildcards are allowed.

Click Save.

See "Creating an Endpoint Discover scan" on page 1389.

See "Using include and exclude filters" on page 1392.

## Using environment variables in Endpoint Discover scans

You can use environment variables to include or exclude file locations regardless of the supported Windows OS version, user profile, or platform of the endpoint. For example, you may want to create an Endpoint Discover target that only scans the

Program Files folder on all endpoints or the Documents folder on all user profiles on all endpoints.

Note: Environment variables are not supported on DLP Agents running on Mac endpoints. See "Using filters to scan Windows and Mac operating systems" on page 1399.

Table 72-6 lists the environment variable types you can use.

**Table 72-6** Environment variable types

Variable type	Element	Description
Operating system defined variable	%	You use this variable type to scan paths specific to the endpoint operating system. For example, you would use <b>%TEMP%</b> to scan the TEMP folder on all targeted endpoints.
Symantec Data Loss Prevention defined variable	\$	You use this variable to scan all user profile paths on a single endpoint. For example, you would use <b>\$Documents\$</b> to scan the <code>Documents</code> folder in all user profiles present on the targeted endpoints.

Variables that include or exclude user profile paths (whether Symantec Data Loss Prevention or operating system defined) are resolved to all the user profiles present on the endpoint. For example, if two user profiles exist on an endpoint, and you specify **\$Documents\$** in the include filter, Symantec Data Loss Prevention scans C:\Users\User1\Documents\ and C:\Users\User2\Documents.

Table 72-7 lists the Symantec Data Loss Prevention defined variables.

**Environment variables Table 72-7** 

Symantec Data Loss Prevention defined variable	Default resolved path
\$CommonAdminTools\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\ Programs\Administrative Tools
\$CommonOEMLinks\$	%ALLUSERSPROFILE%\OEM Links
\$CommonPrograms\$ %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs	
\$CommonStartMenu\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu
\$CommonStartup\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\StartUp
\$CommonTemplates\$	%ALLUSERSPROFILE%\Microsoft\Windows\Templates
\$Cookies\$	%APPDATA%\Microsoft\Windows\Cookies

Environment variables (continued) **Table 72-7** 

Symantec Data Loss Prevention defined variable	Default resolved path	
\$Desktop\$	%USERPROFILE%\Desktop	
\$Documents\$	%USERPROFILE%\Documents	
\$Favorites\$	%USERPROFILE%\Favorites	
\$Fonts\$	%WINDIR%\Fonts	
\$History\$	%LOCALAPPDATA%\Microsoft\Windows\History	
\$InternetCache\$	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files	
\$LocalAppData\$	%LOCALAPPDATA% (or %USERPROFILE%\AppData\Local)	
\$LocalizedResourcesDir\$	%WINDIR%\Resources\0409	
\$Music\$	%USERPROFILE%\Music	
\$NetHood\$	%APPDATA%\Microsoft\Windows\Network Shortcuts	
\$Pictures\$	%USERPROFILE%\Pictures	
\$PrintHood\$	%APPDATA%\Microsoft\Windows\Printer Shortcuts	
\$ProgramData\$	%ProgramData% (or %SystemDrive%\ProgramData)	
\$ProgramFiles\$	%ProgramFiles% (or %SystemDrive%\Program Files)	
\$ProgramFilesCommon\$	%ProgramFiles%\Common Files	
\$ProgramFilesCommonX64\$	%ProgramFiles%\Common Files	
\$ProgramFilesCommonX86\$	%ProgramFiles%\Common Files	
\$ProgramFilesX64\$	%ProgramFiles% (or %SystemDrive%\Program Files)	
\$ProgramFilesX86\$	%ProgramFiles% (or %SystemDrive%\Program Files)	
\$Programs\$	%APPDATA%\Microsoft\Windows\Start Menu\Programs	
\$Public\$	%PUBLIC% (or %SystemDrive%\Users\Public)	
\$PublicDesktop\$	%PUBLIC%\Desktop	
\$PublicDocuments\$	%PUBLIC%\Documents	
\$PublicDownloads\$	%PUBLIC%\Downloads	

Environment variables (continued) **Table 72-7** 

Symantec Data Loss Prevention defined variable	Default resolved path		
\$PublicGameTasks\$	%ALLUSERSPROFILE%\Microsoft\Windows\GameExplorer		
\$PublicMusic\$	%PUBLIC%\Music		
\$PublicPictures\$	%PUBLIC%\Pictures		
\$PublicVideos\$	%PUBLIC%\Videos		
\$Recent\$	%APPDATA%\Microsoft\Windows\Recent		
\$ResourceDir\$	%WINDIR%\Resources		
\$RoamingAppData\$	%USERPROFILE%\AppData\Roaming		
\$SampleMusic\$	%PUBLIC%\Music\Sample Music		
\$SamplePictures\$	%PUBLIC%\Pictures\Sample Pictures		
\$SamplePlaylists\$	%PUBLIC%\Music\Sample Playlists		
\$SampleVideos\$	%PUBLIC%\Videos\Sample Videos		
\$SendTo\$	%APPDATA%\Microsoft\Windows\SendTo		
\$StartMenu\$	%APPDATA%\Microsoft\Windows\Start Menu		
\$Startup\$	%USERSPROFILE%\Microsoft\Windows\Start Menu\Programs\StartUp		
\$System\$	%WINDIR%\system32		
\$SystemX86\$	%WINDIR%\system32		
\$Templates\$	%APPDATA%\Microsoft\Windows\Templates		
\$UserProfiles\$	%SystemDrive%\Users		
\$Videos\$	%USERPROFILE%\Videos		
\$Windows\$	%WINDIR%		

See "Include filter examples" on page 1398.

### Include filter examples

The following section provides an Endpoint Discover include filter example that uses environment variables.

See "Using environment variables in Endpoint Discover scans" on page 1395.

**Table 72-8 Include filter** example

Filter string	Explanation
*.doc, \$Documents\$, >*.company.com, >192.168.32.0/8, >EDT*	The Endpoint Discover scan monitors:  All .doc documents on all fixed drives that are associated with the scan.  All files in the \My Documents\ file path.  All endpoints in the .company.com domain.  All computers on the 192.168.32.0/8 network.  Any endpoints with the WINS name EDT.

## Using filters to scan Windows and Mac operating systems

If you plan to run Endpoint Discover scans on both Windows and Mac endpoints using the same Endpoint Discover scan target, consider exclude and include filter limitations. You can use both filter types to scan Windows endpoints. You can use exclude filters to scan Mac endpoints. However, using exclude and include filters together is not fully supported on Mac endpoints.

The following list provides scan scenarios for Mac endpoints:

- If an include filter is used, Symantec Data Loss Prevention does not scan Mac endpoints.
- If an exclude filter is used, Symantec Data Loss Prevention scans Mac endpoints.
- If an include and exclude filter are both used, Symantec Data Loss Prevention does not scan Mac endpoints.

File path and file type filters are fully supported on both Windows and Mac endpoints. See "Setting up Endpoint Discover filters to include or exclude items from the scan" on page 1395.

The following table illustrates a number of scenarios of how exclude and include filters affect scans on mixed operating system endpoints.

**Table 72-9** Multiple operating system scan scenarios

Scenario	Include filter	Exclude filter	Windows	Мас
Scan all endpoints with the IP range 192.64.110.0/24.	>192.64.110.0/24	None	The endpoint is scanned if it matches the IP filter, otherwise it is not scanned.	The endpoint is not scanned.

Scenario	Include filter	Exclude filter	Windows	Mac
Scan endpoints in the *.company.com domain, and exclude computers in *.test.company.com domain.	>*.company.com	>*.test.company.com	The endpoint is scanned if it is in the test.company.com domain. Endpoints in the .test.company.com domain are not scanned.	The endpoint is not scanned.
Scan all endpoints other than those starting with L_CMP*.	None	>L_CMP*	All endpoints are scanned except for those with names that start with L_CMP.	All endpoints are scanned.
Scan *.txt and *.doc files on IP address 10.216.122.22.	>10.216.122.22,*.txt,*.doc	None	Scans *.txt and *.doc files if the IP address is 10.216.122.22. All other endpoints are not scanned.	The endpoint is not scanned.

**Table 72-9** Multiple operating system scan scenarios (continued)

# Configuring Endpoint Discover scan timeout settings

An Endpoint Discover scan might not complete if one or more endpoints are disconnected and cannot report to the Endpoint Server. The Scan Idle Timeout setting can be configured to stop the Endpoint Discover scan if no endpoints report scan status to the Enforce Server for a specified period of time.

You can configure the Max Scan Duration to define the maximum time duration for an Endpoint Discover scan to run. When an Endpoint Discover scan exceeds the Max Scan Duration, the Endpoint Discover scan stops and displays timeout status.

The Endpoint Discover scan history reports the **Timeout** scan status. To access the scan history, select **Manage** > **Scan History** from the Enforce Server administration console.

#### Configuring the Scan Idle Timeout setting

- Locate Scan Idle Timeout from the Advanced settings tab from the Manage > Discover Scanning > Discover Targets screen.
- Enter the amount of time and select **Minutes** or **Hours**.

The value you enter should exceed the polling interval value (ServerCommunicator.CONNECT\_POLLING\_INTERVAL\_SECONDS.int).

See "Advanced agent settings" on page 1414.

Note: To disable Scan Idle Timeout, select Indefinite for the duration of time.

3 Click Save to save the settings.

#### **Configuring the Max Scan Duration setting**

- Locate Max Scan Duration from the Advanced settings tab.
- 2 Enter the amount of time and select **Minutes**, **Hours**, or **Days**.

Note: To disable Max Scan Duration, select Indefinite for the duration of time.

3 Click **Save** to save the settings.

# Managing Endpoint Discover target scans

After you create and run an Endpoint Discover scan, you can perform a number of management tasks. These tasks can include the following:

- Manage Endpoint Discover in-progress scans. See "About managing Endpoint Discover scans" on page 1401.
- Remediate Endpoint Discover incidents. See "About remediating Endpoint Discover incidents" on page 1402.
- Enabling rules results caching (RRC). See "About rules results caching (RRC)" on page 1403.
- Create endpoint reports. See "About Endpoint reports" on page 1403.

# About managing Endpoint Discover scans

To manage your Endpoint Discover scan targets, you can perform the following:

Start, stop, and pause target scans.

- Monitor status as target scans run.
- Select targets to view details.
- Edit or delete targets.
- Manage multiple targets.
- Sort and filter targets for easier target management.
- Specify the number of targets to display.
- Review scan history See "Managing Network Discover scan histories" on page 1212.
- Manage servers See "Managing Network Discover Servers" on page 1219.
- Review scan status
  - Completed
  - Timeout
  - Stopped
  - Running

See "Scanning new or modified items with differential scans" on page 1225.

- Information about responding to scans See "About remediating Endpoint Discover incidents" on page 1402.
- Information about interpreting scan results and status See "About incident reports for Network Discover" on page 989.

# About remediating Endpoint Discover incidents

Incidents that are created for Endpoint Discover violations display under the Discover tab of the Incidents section. Incidents are marked with an Endpoint-specific icon. You can manually remediate Endpoint Discover incidents using Smart Response rules, use quarantine response rules, or create a custom response using the Endpoint FlexResponse API. See the Symantec Data Loss Prevention Endpoint FlexResponse Plug-in Developers Guide.

See "Endpoint incident lists" on page 964.

You can use the following features to remediate Endpoint Discover incidents:

- Smart Response rules See "About Automated Response rules" on page 881.
- Quarantine response rules

See "About Endpoint Quarantine" on page 1388.

 Endpoint FlexResponse See "About Endpoint FlexResponse" on page 1512.

See "About Endpoint reports" on page 1403.

# About rules results caching (RRC)

Rules results caching (RRC) is a form of pre-detection on the DLP Agent. By caching information about any content that does not match a rule, the DLP Agent can ignore that content. RRC speeds detection because it allows the DLP Agent to only perform detection on new or recently changed content.

Only Described Content Matching (DMC) rule results can be cached in the DLP Agent. Other types of detection, Exact Data Matching (EDM), File Properties Type (FPT), and Indexed Data Matching (IDM) are not applicable to RRC. Additionally, RRC is not applicable to protocol or to group detection rules.

See "Detecting data loss" on page 296.

Any time that the policies that are associated to the DLP Agent change, the RRC cache is deleted. Previous RRC results are cleared and you must scan all of your content again. However, after the initial scan is complete, subsequent scans are much quicker to complete.

By default, RRC is active. If you do not want RRC, go to the advanced agent settings and set it to Off.

# About Endpoint reports

Use incident reports to track and remediate incidents on your endpoints. Symantec Data Loss Prevention reports an incident when it detects data that matches the detection parameters of a policy rule. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches detection parameters is called a match, and a single incident may include any number of individual matches.

Reporting for Endpoint Discover is found under the Discover Reporting section. Endpoint Discover incidents are marked to distinguish them from other types of Discover incidents.

Reporting for Endpoint Prevent is found in the **Reports** tab of the Enforce Server.

You can view the following reports:

- Exec. Summary Endpoint
- Incidents All

- Incidents New
- Policy Summary
- Status Summary
- Highest Offenders

If an incident is created that includes user justifications, those justifications are included in the report in the Incident snapshot section. For example, if a violation occurs that requires the user to enter the response User error, the incident report includes the text SPECIAL: User typed response: "User error".

If the user selects a pre-generated justification, the justification appears in the report. Justifications appear in the detailed report under the header Justifications.

Justifications and notifications are not compatible with Endpoint Discover, therefore no justifications appear in Endpoint Discover reports.

You can also create customized reports for Endpoint Discover and Prevent. However, if the user is not on the network at the time the justification is entered, the justification section of the incident snapshot remains empty.

See "About Symantec Data Loss Prevention reports" on page 1006.

See "How to implement Endpoint Prevent" on page 1378.

See "Setting up and configuring Endpoint Discover" on page 1389.

# Working with agent configurations

This chapter includes the following topics:

- About agent configurations
- Adding agent configurations
- Applying agent configurations to an agent group
- Configuring the agent connection status
- Enabling the communication channel for 12.0.x and earlier agents

# About agent configurations

The **Agent Configuration** page on the Enforce Server administration console lets you configure agent settings.

Each configuration contains configuration options for your agents. These configuration options determine the detection types that occur on endpoints. You can also specify filters and resource consumption limits. You can create as many different agent configurations as you want. However, you cannot delete the default agent configuration. Symantec Data Loss Prevention endpoint protection must contain at least one agent configuration. You can modify the default configuration as many times as you want.

Agent groups can only use one configuration at a time. However you can associate one agent configuration to multiple agent groups. You can also clone agent configurations.

See "Adding agent configurations" on page 1406.

See "About cloning agent configurations" on page 1406.

See "Viewing and managing agent groups" on page 1451.

See "Applying agent configurations to an agent group" on page 1441.

## About cloning agent configurations

You can clone agent configurations. Cloned configurations are identical to the configurations from which they were cloned. Clone agent configurations when you want to keep most of the entity details the same, but need to make small changes. Click the clone icon next to the edit icon to clone a configuration. When you clone a configuration, you see an editable version of that cloned configuration. You must rename the cloned configuration so that you can distinguish between the original and the clone.

The agent configuration page contains information about all of the available agent configurations.

You can also click **Add Configuration** to create new agent configurations.

See "Adding agent configurations" on page 1406.

## Adding agent configurations

You can add or edit agent configurations by going to System > Agents > Agent Configuration and clicking the Add Configuration button.

Create or edit an agent configuration by modifying the following tabs:

- Agent Monitoring
- Agent Configuration
- Advanced Agent Settings

#### Agent Monitoring tab.

Use this tab to select which aspects of the endpoint items you want to monitor. The Agent Monitoring tab is divided into three sections.

■ Enable Monitoring section. Select the endpoint applications and destinations (channels) to monitor.

Destinations Select the destinations to be monitored. Destinations are the physical media or periphery

devices that are attached to the endpoint, such as CD/DVD drives, USB-connected devices, printers, and so on.

Select email applications to be monitored.

Email

Field	Description
Web	Select web applications to be monitored. HTTPS monitoring is only supported for Firefox and Internet Explorer browsers.
Instant Messaging	Select instant messaging applications to be monitored.
Applications	Select to add application file access monitoring.
	See "About monitoring applications" on page 1503.
Network Shares	Select to monitor network shares. You can monitor the files that are transferred to or from your local drive and a network share.

**Filter by File Properties** section. Create and edit monitoring filters. Using this option lets you optimize performance and reduce false positives. Based on the filters you set, the Symantec DLP Agent monitors or ignores data based on protocol, destination, file size, file type, or file path. Existing filters are listed in this section. The filters run in the order they appear in the list as determined by the Order column.

Note: When you filter by file path, the drive letter is ignored and the specified path for every local drive on the agent is filtered. For example, entering c:\temp causes c:\temp and d:\temp to be filtered on an agent with two local drives.

- To create a new filter, click **Add Monitoring Filter**.
- To modify an existing filter, click on the filter in the list.
- To delete an existing filter, click on that filter's red "X."
- To change the order in which a filter is applied, click the filter number in the **Order** column. Then select the execution order for that filter in the drop-down list. Changes are only applied after you click **Save** at the top of the screen.
- Choose either Monitor or Ignore to specify what to do with the files that do not match any of the filters in the Filter by Network Properties section.

See "Configuring file filters" on page 1412.

Create network-related filters that make the agent monitor or ignore network traffic based on IP address or domain. Enter the IP addresses, HTTP domains, and HTTPS domains that you want to filter on in the appropriate box. For filtering IP addresses, use the following rules: Enter any IP-based filters that you want to use. If you leave this field blank, Symantec Data Loss Prevention inspects all packets. The format of the IP protocol filters (found in the protocol definitions and protocol filter definitions) is:

```
ip protocol filter := protocol filter multiple entries [; *]
protocol filter multiple: entroitescol filter entry
                         [; protocol filter multiple entries]
protocol filter entry := +|-|, destination subnet description,
destination subnet description
source subnet description subnet description
subnet description
                     := subnet description
                      := network ip_address / bitmask
                      | *
```

Each stream is evaluated in order against the filter entries until an entry matches the IP parameters of the stream.

A minus sign (-) at the start of the entry indicates that the stream is dropped. A plus sign (+) at the start of the entry indicates that the stream is kept.

A subnet network description of \* means that any packet matches this entry. A subnet bitmask size of 32 means that the entry must match the exact network address. For example, a filter of +,10.67.0.0/16,\*;-,\*,\* matches all streams going to network 10.67.x.x but does not match any other traffic.

Note: The more specific you are when you define the recognition characteristics, the more specific your results. For example, if you define only one specific IP address, only incidents involved that IP address are captured. If you do not define any IP addresses, or if you define a wide range of IP addresses, you achieve broader results. Include at least one plus sign (+) clause and one minus sign (-) clause to be explicit about what is included and what is excluded.

The Domain filters need to be applied separately for HTTP and HTTPS. To add filters for any website that supports HTTP and HTTPS, add individual filters for HTTP and HTTPS in the respective text boxes. The IP address filter works with all other network protocols.

For filtering HTTP/HTTPS domain names, use the following rules:

You can use filters to include (inspect) or exclude (ignore) messages from specific senders. You can also use filters to include or exclude specific recipients. The specific filter syntax depends on the protocol.

The following is an example of domain filters

```
Domain Filter
                   := <Domain Filter Entry> [, <Domain Filter Entry>]
Domain Filter Entry := {*|{-|+}<metadata value>}
```

You can use the following symbols:

- You can use the wildcard symbol (\*) in the domain entry. For example, \*symantec.com would match www.symantec.com, www.dlp.symantec .com, and all domains that end with symantec.com.
- A minus sign (-) at the start of the entry indicates that the URL is ignored.
- A plus sign (+) at the start of the entry indicates that the URL is inspected.
- If you add an asterisk (\*) to the end of the filter expression, any URL domain not explicitly matching any of the filter masks is ignored.

These filters are executed is from left to right until the first match occurs or the agent reaches the end of the filter entries.

For example, if the filter is:

```
-sales.symantec.com, +*symantec.com, *
```

HTTP requests to sales.symantec.com are ignored, and all of the requests that are sent to any other symantec.com domain are inspected. The last asterisk in the filter filters out all other domains like www.xyz.com.

Note: If you leave the HTTP/HTTPS filter empty, all the URLs are inspected.

The filters that you specify with this screen only apply to the individual Endpoint Server where these filters are configured. If you have more than one Endpoint Server, you must individually configure the file filters for each server.

#### Agent Configuration tab.

The **Agent Configuration** tab is divided into the following sections:

Server Communication section.

Set the maximum amount of bandwidth (in megabits or kilobits per second) that a DLP Agent can use to upload data to and download data from the Endpoint Server during connection time.

See "About the DLP Agent store" on page 1414.

The default setting of the consumption throttle is 5 Mbps. To change the bandwidth throttle, select either Mbps or Kbps and then enter a number in the box for the maximum per second. If you leave a field empty, no throttling is applied for that direction of communication traffic.

Field	Description	Agents
From Agent Thottle	Maximum rate at which the DLP Agent uploads incidents, status, events to the Endpoint Server.	Throttle setting applies to all DLP Agent versions.
To Agent Thottle	Maximum rate at which the DLP Agent downloads policy and agent configuration updates from the Endpoint Server.	Throttle setting only applies to 12.5 and later DLP Agent versions.

■ Resource Consumption on the Endpoint Host section.

Use this section to set the maximum disk space for the Agent Store Size. The DLP Agent uses the Agent Store to temporarily store incidents and other data on each endpoint host.

See "About the DLP Agent store" on page 1414.

You can specify a percentage of the hard drive, or a storage limit. Click the appropriate radio button to choose either a percentage of disk space or a storage limit.

Field	Description
% of Total Disk Space limit	For percentage enter the amount in the corresponding box. The default percentage is 5% of total disk space.
Absolute disk space size limit	Select the radio button for this option, enter the particular size in the field, and choose the unit of measurement from the drop-down list (Bytes, KB, MB, or GB).

Resource Consumption for Endpoint Discover Scans section. Use this section to manage resources when Discover scans endpoints:

Note: The long-term average CPU usage and minimum battery life remaining features are not currently supported for agents running on Mac endpoints.

Field	Description
Long-Term Average CPU Usage	Specify the maximum average percent of CPU resources that can be used for Discover scans over a length of time. If the Symantec DLP Agent exceeds this maximum CPU limit, Endpoint Discover detection terminates, but Endpoint Protect detection continues as normal. The default is 20%.
	<b>Note:</b> Any changes you make to the CPU resources threshold should take effect immediately. If you make a change during a scan, the change takes effect after the agent resumes scanning.
Minimum Battery Life Remaining	Specify a minimum amount of the battery that is needed to run your agents. If battery power falls under this minimum, Endpoint Discover detection stops, but Endpoint Protect detection functions normally. The default is 30%.

File Recovery Area Location section. Specify file recovery parameters. File recovery location is where copies of the sensitive data that the DLP Agent blocked from transfer are stored. These copies are kept until recovered by the user, or automatically deleted after a period of time.

Field	Description
File Recovery Area Location	Specify the path to the file recovery directory. The default is ${\tt TMP}\$
Time To Expiration	Specify the amount of time before files are automatically deleted from the file recovery folder. The default is 48 hours.

See "About Symantec Data Loss Prevention administration" on page 55.

See "Server configuration—basic" on page 180.

See "Server controls" on page 178.

#### Advanced Agent Settings tab.

You can also specify advanced settings for the agents. These settings affect how the Symantec DLP Agents process information, detect violations, and perform on endpoints.

Note: Contact Symantec Support before changing any of the advanced settings.

See "Advanced agent settings" on page 1414.

Note: If you modify an existing agent configuration, clicking the Save button applies the changes to all of the agent groups associated with the configuration. If you create a new configuration, the configuration is saved and you can apply it on the Agent Groups screen.

See "About agent configurations" on page 1405.

See "Applying agent configurations to an agent group" on page 1441.

## Configuring file filters

You can configure DLP Agents to monitor specific file types, applications, protocols, or locations. Configuring these items lets you potentially improve monitor performance. You configure the DLP Agent by going to System > Agents > Agent Configuration. You then select an agent configuration you want to configure then click Add Monitoring Filter.

The Configure Server - File Filter filters page is divided into the following three sections:

- Filter Action
- **Endpoint Channel**
- File Attributes

The Filter Action section lets you select whether you want the filter to monitor the following attributes or not. You can include files to be monitored or exclude files from the relevant protocol or destination.

You can select one of the following choices:

- Monitor
- Ignore (do not monitor)

The **Endpoint Channel** section lets you select the destinations, protocols, or applications that you want to filter. You must select at least one option. Select the items that you want the Endpoint Server to monitor.

You can select the following options:

- Removable Storage
- CD/DVD
- Local drive
- Application File Access
- **Email Attachment**

- HTTP/HTTPS Attachment
- IM File transfer
- FTP transfer

The Application File Access option lets you monitor any applications that appear on the Application Monitoring page.

See "About monitoring applications" on page 1503.

The File Attributes section is where you specify the filters that you want to apply. Information you enter in this section applies to local drive and application file access monitoring. Select Local Drive or Applicaton File Access to edit the File Path on Destination field.

You can specify the following filter attributes:

Size

You can specify a minimum, maximum, or baseline size of the files you want to scan.

Type

Specify the exact file types that you want to filter. This section is pre-loaded with common file types. If you specify any additional file types, enter each file type on a separate line.

File Path on Destination

Specify the file-system path(s) to analyze. Enter one path per line. If you specify any paths to include, Symantec Data Loss Prevention monitors only files in those paths. If you leave this field blank, Symantec Data Loss Prevention monitors all files except the files that you may have specified elsewhere. This filter applies to both local drive monitoring and application file access. You can use environment variables to include or exclude file locations regardless of the user profile or platform of the endpoint. For example, if you enter:

%TEMP%

#### \$PublicDownloads\$

Symantec Data Loss Prevention scans the Downloads folder on all user profiles and the Temp folder.

See "Using environment variables in Endpoint Discover scans" on page 1395.

Endpoint monitor filters always run in the order that they appear. If you want to rearrange the run order of the filters, contact Symantec Support. Rearranging the endpoint monitor filter order may cause agents to stop monitoring sensitive information.

See "About agent configurations" on page 1405.

### About the DLP Agent store

When the DLP Agent is not connected to the Endpoint Server, the DLP Agent temporarily stores incidents, two-tier detection requests, and response actions locally on the endpoint host. The DLP Agent stores incident and detection metadata, and response action data and metadata, in a small encrypted database that is installed with the DLP Agent. The DLP Agent stores incident data and content for two-tier detection requests on the endpoint host file system. This data is encrypted and the encryption key is stored in the agent database.

The **Agent Store Size** parameter limits the amount of data that the DLP Agent stores on the endpoint host. The default agent store size is 5% of total disk space. Alternatively, you can set an absolute storage limit. The Agent Store Size limit applies to all data stored on the endpoint host, including data stored in the agent database and data stored on the host file system

If the Agent Store Size limit is exceeded, the DLP Agent deletes data from the endpoint host according to a set priority until the Agent Store Size limit is no longer exceeded. If the DLP Agent must delete incidents, the order of eviction is as follows:

- 1) Two-tier detection request data (oldest first)
- 2) Endpoint Discover incidents (oldest first)
- 3) Endpoint Prevent incidents (oldest first)

See "Adding agent configurations" on page 1406.

## Advanced agent settings

The following settings affect only the Symantec DLP Agent. These settings should not be modified without the assistance of Symantec Support. If you want to make modifications to this screen, please contact Symantec Support before making any changes.

Table 73-1 provides a list of agent settings, along with the default value and description of each setting.

Note: If you change advanced agent settings and the agents connect to Endpoint Servers in a load-balanced environment, you must apply the same changes to all Endpoint Servers in the load-balanced environment.

**Table 73-1** Agent advanced settings

Name of Setting	Default values	Description
AgentManagement.DISABLE_ENABLE_TASK_TIMEOUT_SECONDS.int	300	The amount of time, in seconds, the Disable or Enable agent troubleshooting task waits before it sends the Agent Requires Restart system event.
AgentTamperProtection.ENABLE_AGENT_ TAMPER_PROTECTION.int	7	This setting enables tamper protection on the Symantec Data Loss Prevention Endpoint agent.  A setting of 0 disables all tamper protection.
		A setting of 1 prevents the agent and the watchdog files from being deleted or modified.
		A setting of 2 prevents the agent and the watchdog services from being stopped.
		A setting of 3 prevents the agent and the watchdog files and services from being deleted, modified or stopped.
		A setting of 4 prevents the agent and the watchdog services from being deleted from the operating-system registry.
		A setting of 7 enables file, service, and registry protection.
AgentThreadPool.IDLE_TIME_IN_SECONDS.int	60	The maximum time a thread can be inactive before it is removed from the thread pool. Threads are also known as agent tasks.
AgentThreadPool.MAX_CAPACITY.int	20	The maximum number of threads in the thread pool. The threads can be either active or inactive.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
AgentThreadPool.MIN_CAPACITY.int	2	The minimum number of threads that are allowed in the thread pool. The thread pool must always contain this number of threads. The threads can be either active or inactive.
AggregatorCommunicator.ENABLE_ENDPOINT_ DATAFLOW_CACHING.int	1	If enabled (1), this setting prevents agent from downloading data, like policies and configuration files, that have already been downloaded. Enter <b>0</b> to disable this setting.
ApplicationConnector.KEY_LENGTH.int	64	The length of the key, in bytes, that is used to obfuscate communication between the agent and the application hooks.
ApplicationConnector.MAX_CONNECTIONS.int	255	The maximum number of application hooks (per type of hook) that can simultaneously connect to the agent.
ApplicationConnector.TEMPORARY_DIRECTORY.str	%TMP%	The temporary location where application hooks store obfuscated content.
AttributeResolver.ATTRIBUTE_REFRESH_INTERVAL_IN_DAY.int	7	The number of days the agent waits to refresh Active Directory attribute information. If the agent finds the information that is older than the number of days indicated, then contacts contacts the Active Directory server. If value is set to 0, the agent does not contact AD server to retrieve attribute information.
ClipboardViewer.SLEEP_TIME_IN_MS.int	10	The time delay, in milliseconds, before the agent fetches contends from the endpoint clipboard.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
CommLayer.MAX_FRAME_SIZE_KILOBYTES.int	8	The maximum size of each outbound frame. This is the maximum number of kilobytes per frame read from the applications.  Changes to this setting apply to all new connections. Changes do not affect existing connections.
CommLayer.NO_TRAFFIC_TIMEOUT_SECONDS.int	300 seconds (5 minutes)	The application level heartbeat interval. To detect idle dead connections the agent uses an application level heartbeat message. Data Loss Prevention closes the connection for which a heartbeat has not been received in the specified timeout interval. The agent does not send heartbeats and relies on the TCP keepalive instead. A 0 value indicates that the heartbeat should be disabled. This value is also used as an application handshake timeout value.  Changes to this setting apply to existing and new connections.  You can enter a value between 60 and 86400 seconds.
ComponentLoaderSettings.MAX_ COMPONENT_SHUTDOWN_TIME.int	60000	The maximum amount of time, in milliseconds, that the agent waits for a component to shut down.
ComponentLoaderSettings.PROCESS_PRIORITY.str	NORMAL	The priority level that dictates what priority the DLP Agent runs on the endpoint. You can also enter NORMAL and ABOVE_NORMAL.

**Table 73-1** Agent advanced settings (continued)

N 66 W			
Name of Setting	Default values	Description	
CrashDump.ENABLE_CRASH_DUMP_COLLECTION.int	1	The setting that allows the system to create a dump file when the Symantec DLP Agent crashes. Setting this value to 1 enables the crash dump file to be created. Enter 0 to disable the file.	
CrashDump.MAX_DAYS_TO_KEEP_DUMP.int	2	The maximum time, in days, that the crash dump file is stored.	
CrashDump.MAX_NUMBER_OF_FILES_IN_DUMP_FOLDER.ii	nt 3	The maximum number of files to keep in the crash dump folder.	
Detection.CHUNK_OVERLAP.int	45	The number of characters each chunk borrows from the end of the previous chunk.	
Detection.CHUNK_SIZE.int	65536	The text chunk size in bytes.	
Detection.DAR_KVOOP_PRIORITY.str	BELOW_NORMAL	The priority of the external kvoop process while it extracts text for Endpoint Discover scans.	
Detection.ENABLE_METADATA.str	off	Allows detection on file metadata when a user attempts to transfer or print a file. If the setting is turned on, you can detect metadata for Microsoft Office and PDF files. For Microsoft Office files, OLE metadata is supported, which includes the fields Title, Subject, Author, and Keywords. For PDF files, only Document Information Dictionary metadata is supported, which includes fields such as Author, Title, Subject, Creation, and Update dates. Extensible Metadata Platform (XMP) content is not detected. Enabling this option can cause false positives.	

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
Detection.FILTER_TIMEOUT.int	420000	The time limit, in milliseconds, for filtering text.
Detection.LOCAL_DRIVE_KVOOP_PRIORITY.str	BELOW_NORMAL	The priority of the external kvoop process while it extracts text for local drive events.
Detection.MARKUP_AS_TEXT.str	off	Stops the detection on any text that has XML or HTML tags associated with it.
Detection.MAX_DETECTION_TIME.int	900000	The maximum amount of time to complete endpoint detection in milliseconds.
Detection.MAX_FILTER_FILE_SIZE.int	31457280	Maximum file size for text filtering in bytes.
Detection.MAX_IDM_FILE_SIZE	31457280	Maximum file size for IDM content extraction.
Detection.MAX_NUM_MATCHES.int	300	Maximum number of matches for a given matcher.
Detection.MAX_QUEUE_SIZE.int	10000	The maximum number of items that simultaneously wait for detection.
Detection.MIN_EXTRACTED_CHARS_FOR_TEXT_IDM_MATCH	30	Minimum size of the normalized content before the cracked content will be indexed, otherwise an exact match will be performed against the raw (binary) content. Must match the min_normalized_size parameter in the Indexer.properties file.
Detection.NEWLINE_ELIMINATION.str	on	Sets whether newlines are eliminated before detection.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
Detection.RULESRESULTSCACHE_ENABLED.str	on	Rules results caching (RRC) is a way to cache the results of content on a Symantec DLP Agent that does not violate a policy.
		See "About rules results caching (RRC)" on page 1403.
		By default, RRC is set to on. If you do not want to use RRC, set this parameter to off.
Detection.RULESRESULTSCACHE_FAST_CACHE_SIZE.int	1024	The size of the rules results caching first-level database, the Level 1 database. Rules results caching sends new entries of recorded, non-violating files to the Level 1 database. After the Level 1 database is full, entries are flushed to the Level 2 database to maintain the space of the Level 1 database.
Detection.SHORT_DAR_DETECTION_TIME.int	2000	The amount of time, in milliseconds, taken to detect on a file before the file is considered too large.
Detection.TRACKED.CHANGES.str	off	Allows the detection of content that has changed over time (Track Changes content) in Microsoft Office documents. Using this option might reduce the accuracy rate for IDM and data identifiers.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
Detection.TWO_TIER_IDM_ENABLED.str	See descritpion	Enables two-tier detection for IDM for the DLP Agent. Set to "off" to use exact match IDM on the endpoint. Set to "on" to use two-tier detection.
		For new installations the default is set to "off" so that by default the DLP Agent uses exact match IDM on the endpoint.
		For upgrades the default is set to "on" so that there is no change in functionality for existing IDM policies deployed to the endpoint.
		See "Using agent IDM after upgrade to version 12.5" on page 494.
Detection.UNICODE_NORMALIZATION.str	on	Transforms the specific characters to UNICODE before detection. This transformation is necessary for matching policies containing data in many Asian languages.
Discover.CRAWLER_THREAD_PRIORITY.str	BELOW_NORMAL	The priority of the Discover threads while drives are scanned.
Discover.POST_SCAN_REPORT_INTERVAL.int	60000	The interval of time, in milliseconds, between two Endpoint Discover status reports. Occurs after the agent has reached end of scan but before the overall scan is finished or aborted.
		This setting only applies to 12.0.x and earlier agents.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
Discover.SCAN_ONLY_WHEN_IDLE.int	2	Sets whether the agent performs an Endpoint Discover scan while the endpoint user is idle.
		If set to 1, the agent only performs Endpoint Discover scanning while the endpoint user is idle.
		If set to 2, the agent only scans small files while the endpoint is active and larger files while the endpoint user is idle. Files taking longer than DetectionSHORT_DAR_DETECTION_TIME seconds are considered large.
		If set to 0, the scan runs regardless of user activity.
Discover.SECONDS_UNTIL_IDLE.int	120	If the agent does not detect any user activity in this amount of time, in seconds, the user is considered to be idle. Very small amounts of time, less than 60 seconds, may not be precisely adhered to.
Discover.STANDARD_REPORT_INTERVAL.int	60000	The interval of time between two Endpoint Discover scan status reports, in milliseconds.
		To create a transient connection between the agent and Endpoint Server, enter an interval greater than the EndpointCommunications.  IDLE_TIMEOUT_IN_SECONDS.int value.

Agent advanced settings (continued) Table 73-1

Table 73-1 Agent advance	nt advanced settings (continued)		
Name of Setting	Default values	Description	
EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int	270	Time interval in seconds between heartbeat messages.	
		The Endpoint Server sends heartbeat messages to detect dead connections to individual agents when no other traffic is being sent or received. The Endpoint Server measures the time between when the last data traffic was sent to or received by the agent until the current time.	
		Data traffic is defined as any bytes sent or received by the Endpoint Server, including heartbeat message bytes. When the specified duration is exceeded, the Endpoint Server sends a heartbeat message to the agent. If the value of the setting in the agent configuration changes, the new value is applied immediately to any connections that are open to agents for which the configuration applies, and to any subsequent connections.	
		Note: Application-defined heartbeat messages are treated by network appliances as actual traffic and, unlike TCP keepalives, are never ignored. Heartbeat messages do not count as normal messages for the purpose of determining whether the connection is idle. Sending or receiving a heartbeat message does not reset the idle timer.	
		1000000000. Enter 0 to disable the agent heartbeat.	

**Table 73-1** Agent advanced settings (continued)

Agent advanced Settings (continued)		
Name of Setting	Default values	Description
${\bf Endpoint Communications. IDLE\_TIMEOUT\_IN\_SECONDS. int}$	30	The maximum time to keep an idle connection open.
		The connection is closed when the specified number of seconds has passed.
		This timeout only applies during the normal operation phase of a connection. This occurs after the SSL handshake and application handshake phases.
		Enter a value between 0 and 10000000000. Enter 0 to prevent idle connections from closing.
FileService.MAX_CACHE_SIZE.int	250	The maximum number of recently opened file paths that have been recorded for each endpoint process.
FileSystem.DRIVER_FILE_OPEN_REQUEST_TIMEOUT.int	10	Lets you configure the timeout value, in seconds, for a file open request that is sent from a driver to the agent. This setting is helpful in case the file system connector is slow in responding to the driver. If the connection is slow, the system performs badly. Each file open request is postponed by the driver waiting for the agent to respond. You cannot leave this setting blank and a value of 0 is not allowed.
FileSystem.ENABLE_FILE_RESTORATION.int	1	This setting provides the ability to turn on or turn off file restoration. File restoration is the ability to restore the original file in case it is overwritten with a newer file containing confidential data. File restoration is enabled by default. Enter 0 to disable this setting.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
FileSystem.ENABLE_VEP_FILE_ELIMINATION.int	3	

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
		When the setting is enabled, the system does not create a .vep file. Instead it runs detection on the original file and resolves any sharing violations for EDPA.exe and KVOOP.exe, when needed.
		<b>Note:</b> Enable this setting if your environment does not contain any of the following:
		<ul> <li>Data retention policies</li> <li>Two-tier detection policies</li> <li>Endpoint Discover or Endpoint Prevent encryption software</li> </ul>
		You can use the following values:
		<ul> <li>0 creates a .vep file for all channels.</li> <li>1 runs detection on the original file. A .vep file is created for scanned files that are moved to removable drives.</li> <li>2 runs detection on files moving through the application file access channel. A .vep file is created for all scanned files.</li> <li>3 runs detection on files moving through the application file access and removable channels. A .vep file is created for all other scanned files.</li> <li>4 runs detection on files moving through network shares. A .vep file is created for all other scanned files.</li> <li>5 runs detection on files moving through network shares and removable drives. A .vep file is created for all</li> </ul>

Agent advanced settings (continued) Table 73-1

Name of Setting	Default values	Description
		other scanned files.  6 runs detection on files moving through application file access and network shares.  A .vep file is created for all other scanned files.  7 runs detection on files moving through removable drives, application file access, and network shares. A .vep file is created for all other scanned files.
FileSystem.IGNORE_STORAGE_BUS_TYPE.int	None	This setting controls whether storage devices are ignored or not. Enter None to monitor all storage devices. Enter All to ignore all removable devices.
FileSystem.MAX_BACKLOG	20	The maximum number of snapshot files that are created when removable storage is monitored.
FileSystem.MONITOR_APPLICATION_CHILD_ PROCESS_FILE_ACCESS.INT	1	This setting allows the user to enable or disable the Application File Access feature that monitors child processes. Enter 1 to enable or enter 0 to disable.
FileSystem.NUM_OF_LISTENER_THREADS	1	The number of listener threads that listen to file system driver requests. You can enter any positive integer value.
FileSystem.NUM_TIMES_TO_OVERWRITE_FILE.int	2	This setting indicates how many times a file is overwritten with a secure pattern before it is deleted during prevention. A value of 0 indicates that the file cannot be overwritten.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
FileSystem.THREAD_POOL_MAX_CAPACITY	20	The maximum number of threads that the filesystem threadpool can use to serve file system requests.
FileSystem.USE_CDDVD_DEFAULT_EXCLUDE_PATHS.int	1	This setting allows user to exclude any file that is opened by a CD/DVD application from the following directories:  Installed directory of the application; for example, if the application is Roxio, then c:\program files\roxio  System directories; for
		example, %windir%\system32 • Program Files\Common Files  It is enabled by default.
FlexResponse.MAX_INCIDENT_FILE_SIZE.int	31457280	Reserved for future use.
FlexResponse.PLUGIN_HOST_LOG_MAXFILE_SIZE.long	5120000	The maximum size of a plug-in log file. The default number is in bytes.
FlexResponse.PLUGIN_HOST_LOG_MAX_NUMBER_OF_FILES.long	1	The maximum number of plug-in log files that can be kept.
FlexResponse.PLUGIN_HOST_MESSAGE_TIMEOUT.long	180000	The amount of time that the plug-in host can process messages. The default time is in milliseconds.
FlexResponse.PLUGIN_HOST_STARTUP_TIMEOUT.long	30000	The amount of time that the plug-in host can take to start up. The default time is in milliseconds. If the plug-in host does not start in the specified amount of time, the plug-in host sends a fail event to the log.
FlexResponse.PLUGIN_QUEUE_LIMIT	100	The number of FlexResponse plugin invocation requests placed in queue.

**Table 73-1** Agent advanced settings (continued)

Table 7.5-1 Agent advanced settings (continued)		
Name of Setting	Default values	Description
GroupResolution.DAYS_DATA_STALING.int	7	The amount of time, in days, that the agent retains Active Directory (AD) user group information. Information that is older than this limit causes the agent to contact the AD server.
Hooking .APPLICATION_LOAD_TIMEOUT.int	300000	Specifies the time, in milliseconds, that the agent tries to hook into an application if that application takes a long time to load.
Hooking.EXPLORER_APPLICATION_HOOKING.int	1	Allows the DLP Agent to monitor when a user performs a right-click print through Windows Explorer. To turn off right-click print monitoring, change this setting to 0.
Hooking.EXPLORER_HOOKING.int	3	Allows the DLP Agent to monitor Microsoft Windows Explorer traffic.
Hooking .USE_LOADLIBRARYW_FROM_IMAGE.int	0	The method to find the LoadLibraryW function address. You can specify a value of either 0 or 1.  0 uses the GetProcAddress API to find the library.  1 reads the exports table of kernel32.dll to find the library.
IE8_HTTPS.Monitor.int	1	Sets Internet Explorer 8 HTTPS monitoring for Symantec DLP Agents. Internet Explorer 8 HTTPS monitoring for the Symantec DLP Agent is automatic. Monitoring is turned on by default. To turn off Internet Explorer 8 monitoring, change this setting to 0.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
IncidentHandler.CACHE_SIZE_THRESHOLD.int	30	The percentage of used endpoint database cache space that triggers Endpoint Discover to pause.
IncidentHandler.MAX_BACKOFF.int	3600000	Maximum time, in milliseconds, to wait before it retries to send an incident to the server if the first attempt fails.
IncidentHandler.MAX_INCIDENT_FILE_SIZE	31457280	Size, in bytes, of the largest file to be sent from the agent as part of an incident.
IncidentHandler.MAX_TTD_FILE_SIZE	31457280	Size, in bytes, of the largest file to be sent from agent for two-tier detection.
IncidentHandler.MIN_BACKOFF.int	30000	Minimum time, in milliseconds, to wait before the agent re-sends an incident to the Endpoint Server after the first attempt fails.
IncidentHandler.PERSISTER_MAX_DAR_ENTRIES.int	5	The maximum number of persisted Endpoint Discover incidents that are kept in queue.
IncidentHandler.PERSISTER_MAX_ENTRIES.int	25	The maximum limit of incidents in the Agent Store before the agent starts evicting incidents.
IncidentHandler.SENDER_CHUNK_SIZE.int	65536	Size, in bytes, of chunks to read from the database as it sends files.
Logging.OperationLogFileSize.long	5120000	The size of the operational log file. This setting specifies how large, in bytes, each operational log can be. Logs that exceed this setting are not retained.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
Logging.OperationLogMaxFiles.int	30	The maximum number of operation logs, per scan, that are retained at any one time. If this number is exceeded, operational log files are purged from the folder until the limit is reached. Log files are purged according to the date that they were created. The oldest log files are purged first. This setting is not applicable to the entire directory.
Logging.OperationLogTTL.int	90	The number of days that operational logs are kept in the directory. If the operational log is not accessed or modified in the specified number of days, the file is deleted.
MonitorSystemUsers.CLIPBOARD.int	0	Enables system user monitoring for Clipboard feature. Set to inactive by default. Set to 1 to enable.
MonitorSystemUsers.LOCAL_DRIVE.int	0	Enables system user monitoring for the local drive feature. Set to inactive by default. Set to 1 to enable.
MonitorSystemUsers.NETWORK.int	0	Enables system user monitoring for network protocols in the driver (HTTP, FTP). Set to inactive by default. Set to 1 to enable.
MonitorSystemUsers.PRINT_FAX.int	0	Enables system user monitoring for print/fax feature. By default, this feature is set to inactive. Set to 1 to enable.
NetworkMonitor.ENABLE_HTTP_GET_MONITORING.int	0	Enables HTTP/HTTPS GET request monitoring. By default, this setting is disabled. Set to 1 to enable.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
NetworkMonitor.HTTP_DETECTION_TIMEOUT.int	120	The length of time, in seconds, that the agent waits during a scan of HTTP and HTTPS data.
NetworkMonitor.IM_DETECTION_SESSION_TIMEOUT.int	120	The duration, in seconds, of the detection session window for all instant messaging clients.
PluginInstaller.TAMPERPROOFING_ IGNORE_PROCESS_TIMEOUT.int	15000	Lets you specify a time, in milliseconds, to ignore any short-lived processes that do not load plug-ins. If the process ends before this time limit is reached, the plug-in installer does not start.
PostProcessor.ENABLE_FLEXRESPONSE.int	0	Lets you enable or disable Endpoint FlexResponse capability. By default, Endpoint FlexResponse is turned off. Change the setting to 1 to enable Endpoint FlexResponse.
PostProcessor.FILE_SYSTEM_USER_RESPONSE_TIMEOUT.int	60	The amount of time, in seconds, that endpoint users have to select a response action to the User Cancel pop-up notification. This setting only applies to events that are generated by attempting to transfer files that violate a policy.
PostProcessor.NETWORK_USER_RESPONSE_TIMEOUT.int	60	The amount of time, in seconds, that endpoint users have to select a response action to the User Cancel pop-up notification. This setting applies to HTTP, FTP, and IM events only.
PostProcessor.NOTIFY_ON_FIXED_DRIVE.int	0	Enables the response notifications for fixed-drive incidents. The default is set to disable notifications. Set to 1 to enable.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
PostProcessor.NOTIFY_WITH_CANCEL_DEFAULT_ACTION	1	The default action to take if an endpoint user does not select the action from the User Cancel pop-up notification within the specified time. Enter 1 to block the action or enter 0 to allow the action.
PostProcessor.OTHER_USER_RESPONSE_TIMEOUT	60	The amount of time, in seconds, that endpoint users have to select a response action to the User Cancel pop-up notification. This setting only applies to Clipboard, Print, Email, and HTTPS events.
Quarantine.MAX_QUEUE_SIZE.int	100	The maximum number of quarantine requests that can be in the queue at any one time. Requests that exceed this number are dropped and are not quarantined.
ResponseCache.AFAC_TIMEOUT	10000	The amount of time that an application file access incident is cached. Duplicate incidents that occur during this time period are not generated and do not trigger response rule messages.
ResponseCache.CD_TIMEOUT.int	2000	The amount of time, in milliseconds, that a CD/DVD incident is cached. Duplicate incidents within this time period are not generated or cause Prevent pop-up notifications.
ResponseCache.FTP_TIMEOUT.int	10000	The amount of time, in milliseconds, that an FTP incident is cached. Duplicate incidents within this time period are not generated or cause Prevent pop-up notifications.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
ResponseCache.HTTP_TIMEOUT.int	2000	The amount of time, in milliseconds, that an HTTP/HTTPS incident is cached. Duplicate incidents within this time period are not generated or cause Prevent pop-up notifications.
ResponseCache.MAX_SIZE.int	100	The maximum number of incidents that are cached at any time.
ServerCommunication.CONNECTION_ INTERVAL_SECONDS.int	86400	This setting only applies to 12.0.x and earlier agents.
ServerCommunication.CONNECTION_ RETRY_ATTEMPTS.int	10	This setting only applies to 12.0.x and earlier agents.
ServerCommunication.CONNECTION_ RETRY_INTERVAL_SECONDS.int	10	This setting only applies to 12.0.x and earlier agents.
ServerCommunication.CONNECT_WHEN_IP_CHANGES.int	1	This setting only applies to 12.0.x and earlier agents.
ServerCommunicator.CONNECT_ BACKOFF_DURATION_MULTIPLIER.int	2	The factor by which each the last backoff period is multiplied.
ServerCommunicator.CONNECT_ POLLING_INTERVAL_SECONDS.int	900	The amount of time, in seconds, that the agent waits before it initiates connections.  The minimum value you enter depends on the minimum time difference between when the Enforce Server and Endpoint Server communicate. Entering 10 is the minimum value you can enter to maintain a persistent connection. You can enter a value between 60 and 86400 seconds to maintain a non persistent connection.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
ServerCommunicator.INITIAL_ CONNECT_BACKOFF_DURATION_SECONDS.int	30	The duration of time, in seconds, that the agent should backoff after the first backoff error.
		Enter a value less than the ServerCommunicator.MAX_CONNECT_BACKOFF_DURATION_SECONDS.int value.
ServerCommunicator.MAX_ CONNECT_BACKOFF_DURATION_SECONDS.int	1800	The maximum duration of time, in seconds, that an agent should spend in back off before it fails over to the next server.
		You can enter a value between 60 and 86400 seconds.
ServerRedundancy.FAILOVER_INTERVAL.long	3600	Interval of time, in seconds, an agent spends trying to connect to an Endpoint Server before it tries to failover to a new Endpoint Server.
ServerRedundancy.MAX_TIME_ BETWEEN_CONNECTION_ATTEMPTS.long	600	The maximum amount of time, in seconds, the agent waits between connection retries to the same Endpoint Server.
Transport.ALLOW_EXPIRED_CERTIFICATES.int	1	Controls whether or not expired certificates are accepted.
		This setting applied to all new agent connections.
Transport.AUTO_FLUSH_LIMIT_KILOBYTES.int	16	The maximum amount of outbound data, in kilobytes, to enqueue for a connection before auto-flushing.
		Enter a value less than the Transport.MAX_OUTBOUND_ KILOBYTES_TO_BUFFER.int value.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
Transport.DNS_HOST_CACHE_TIMEOUT_SECONDS.int	86,400	The timeout in seconds for DNS host cache. Name resolves are kept in memory for this number of seconds. Set to zero to completely disable caching, or set to -1 to save all cached entries.
		This setting applies to all new agent connections.
		You can enter a value between -1 and 604800 seconds.
Transport.MAX_CONNECT_WAIT_SECONDS.int	30	The time in seconds to wait for the connect call to succeed.
		This setting applies to all new agent connections.
		You can enter a value between 1 and 300 seconds.
Transport.MAX_INBOUND_KILOBYTES_TO_BUFFER.int	100	The maximum of inbound data, in kilobytes, to enqueue for a connection.
		You can enter a value between 16 and 2048.
Transport.MAX_OUTBOUND_KILOBYTES_TO_BUFFER.int	100	The maximum amount of outbound data, in kilobytes, to queue for a connection.
		You can enter a value between 16 and 2048.
		Enter a value greater than the CommLayer.MAX_FRAME _SIZE_KILOBYTES.int value.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
Transport.MAX_SSL_SESSION_LIFETIME_SECONDS.int	86,400	The time duration in seconds for which agent re-uses an SSL session ID. When the duration equal to the configured value elapses, the SSL session ID is discarded by the agent and a new SSL session is established on the subsequent connection with the Endpoint Server.  This setting applies to new agent connections.  Enter 0 to disable SSL re-use.
Transport.VERIFY_SERVER_HOSTNAME	0	When enabled, the Enforce Server verifies the server distinguished or common name mentioned in the server certificate during the SSL handshake process. This setting applies to new connections. Enter 1 to enable and 0 to disable.
UI.BUTTON_OK.str	ОК	Controls the text on the <b>OK</b> button on the user-facing notification message. Change this setting if you use a locale that is not supported. The default language is English.
UI.BUTTON_OKTOALL.str	OK To All	Controls the text on the <b>OK To All</b> button on the user-facing notification message. Change this setting if you use a locale that is not supported. The default language is English.
UI.CONSECUTIVE_TRANSACTION_TIME.str	10	Maximum time, in seconds, between two file operations to be considered as a single transaction.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
UI.MONITOR_MSG_TITLE.str		The message title for a notification pop-up message.
UI.MONITOR_TITLEBAR.str	Warning	Controls the static title message in the title bar for the Endpoint Notify notification pop-up message. Change this setting if you use a locale that is not supported. The default setting is Warning.
UI.NOTIFY_CANCEL_MSG_TITLE	Blank	Enter text here to customize the User Cancel response rule message title.
UI.NOTIFY_CANCEL_TITLEBAR	Blank	Enter text here to customize the User Cancel response rule dialog title.
UI.NO_SCAN.int	0	If any number other than zero, the scan dialog does not display.
UI.NWC_EVENT_LIMIT_FS.int	5	The maximum number of events that can be queued before a default action for further incidents is accepted. This setting applies to File System events only.
UI.NWC_EVENT_LIMIT_NW.int	2	The maximum number of events that can be queued before a default action for further incidents is accepted. This setting applies to Network events only.
UI.POPUP_QUEUE_LIMIT.int	100	The limit of pop-up notifications that a user sees in a single session. These pop-up notifications require a user justification for the validation. If the limit is exceeded, any pop-up notifications past the limit automatically contain a Not Applicable (N/A) justification.

Agent advanced settings (continued) **Table 73-1** 

Name of Setting	Default values	Description
	Delault values	•
UI.PREVENT_MSG_TITLE.str		Message title for a block pop-up message.
UI.PREVENT_TIMEOUT.int	300	Timeout value, in seconds, before the incident is generated. If this limit is exceeded, the incident is created regardless of what the user chooses from the pop-up window.
UI.PREVENT_TITLEBAR.str	Blocked	Controls the static title message in the title bar for the Endpoint block notification pop-up dialog box.
UI.PREVENT_WINPOSITION.int	0	Start position of the Prevent dialog window.
UI.QUARANTINE_PROMPT.str	The file is quarantined at:	Controls the text that specifies where the quarantined data is located.
UI.SCAN_BAR.str	(blank)	This setting lets you change the text in the body of the scan window. This text is static and appears regardless of the locale of the endpoint.
UI.SCAN_DELAY.int	0	The amount of time, in seconds, that occurs before the scan dialog window is displayed.
UI.SCAN_EMAIL.int	0	This setting activates the toggle for email scanning. If this setting is set to 0, users cannot select email monitoring.
UI.SCAN_FTP.int	0	This setting activates the toggle for FTP scanning. If this setting is set to 0, users cannot select FTP monitoring.

**Table 73-1** Agent advanced settings (continued)

Name of Setting	Default values	Description
UI.SCAN_HTTP.int	0	This setting activates the toggle for HTTP monitoring. If this setting is set to 0, users cannot select HTTP monitoring.
UI.SCAN_IM.int	0	This setting activates the toggle for instant message (IM) scanning. If this setting is set to 0, users cannot select IM monitoring.
UI.SCAN_PRINTFAX.int	0	This setting activates the toggle for Print/Fax scanning. If this setting is set to 0, users cannot select Print/Fax monitoring.
UI.SCAN_REMOVABLEMEDIA.int	1	This setting activates the toggle for removable media scanning. If this setting is set to 0, users do not have the option of selecting removable media monitoring.
UI.SCAN_SHOWTIME.int	2	Minimum time, in seconds, for the scan dialog to remain on the screen.
UI.SCAN_TITLE.str	(blank)	This setting lets you enter the title of the scan window that appears for the user. This title is a static message that appears regardless of the locale of the endpoint.
UI.USERINPUT_PROMPT.str	Others:	Controls the prompt that appears in the block and notify pop-up messages at the user input field. Change this prompt if you use a locale that is not supported. The default setting is in English.
UninstallPassword.RETRY_LIMIT.int	3	Defines the number of times a user can attempt to uninstall the DLP agent without entering the correct uninstall password.

## Applying agent configurations to an agent group

You can apply any agent configuration to any agent group. Use the **Apply Configuration** page to assign agent configurations to your agent groups.

See "About agent configurations" on page 1405.

Applying an agent configuration to an agent group

- 1 Go to the **System > Agents > Agent Configuration** screen.
- Click the **Apply Configuration** button

The Agent Groups screen displays. When this screen displays, you assign the agent configuration to an agent group to finish applying the agent configuration.

See "Updating outdated agent configurations" on page 1453.

See "Adding agent configurations" on page 1406.

See "Endpoint Server—basic configuration" on page 191.

## Configuring the agent connection status

You can set the connection period for agents to specify how long they report. Settings you make on this screen apply to all registered Endpoint Servers. The default setting is 18 hours.

Note: The setting you enter should be 5 minutes greater than the agent polling interval (ServerCommunicator.CONNECT\_POLLING\_INTERVAL\_SECONDS.int). See "Advanced agent settings" on page 1414.

#### To configure the agent connection status

- Go to System >Settings >General
- 2 Click Configure.
- Locate the **Agent Connection Status Configuration** area.
- Enter hours and minutes to specify how much time passes before an agent displays as not reporting.
- 5 Save your changes.

## Enabling the communication channel for 12.0.x and earlier agents

You enable communication between the Endpoint Server and 12.0.x and earlier agents by enabling the communication channel. If you have 12.0.x and earlier agents already installed, and you upgrade Symantec Data Loss Prevention to the latest version, the communication channel for 12.0.x and earlier agents is automatically enabled.

To enable the communication channel for 12.0.x and earlier agents

- 1 Go to System > Settings > General
- 2 Click Configure.
- 3 Select the Enable item under the Communication Channel for 12.0.x and Earlier Agents section.
- Save your changes.

# Working with Agent Groups

This chapter includes the following topics:

- About agent groups
- Developing a strategy for deploying Agent Groups
- Overview of the agent group deployment process
- Migrating pre-12.5 Endpoint deployments to agent groups
- Creating and managing agent attributes
- Viewing and managing agent groups
- Viewing group conflicts
- Changing groups

## About agent groups

Agent Groups enable you to group and configure agents according to user-specific or machine-specific characteristics, such as country, location, or department name. These characteristics are called agent attributes. You can use attributes to create groups and assign specific configurations to the groups based on your business needs. Agent Groups can be used to deploy and manage a large number of agents. You can also use Agent Groups to temporarily exempt certain agents, based on attributes, from policies that affect other configurations, for testing purposes.

One Endpoint Server can support multiple Agent Groups. An Endpoint Server can dynamically discover to which agent group a particular agent belongs, based on agent group definitions and agent attributes, and assign the configuration to an agent belonging to the appropriate agent group. Assigning one agent configuration per Endpoint Server is also supported by having a group for the Endpoint Server.

With Agent Groups, attributes of logged-in users and endpoint computers can be used to create group conditions. Symantec Data Loss Prevention provides six predefined attributes. You can create other user-defined attributes based on Active Directory attributes. For example, you can create a group condition based on a location attribute, such as all users (agents) located in New York, and a department attribute, such all users who are part of the Human Resources department. For that group you can deploy a configuration in which removable storage is monitored. In this example, the Agent Group definition has two conditions: location(s) and department name(s).

Agent groups simplify the management of agent configuration exceptions by allowing a logical grouping of endpoint agents based on conditions. For example, if you have Instant Messenger monitoring enabled for US employees, except for those US employees in the state of Texas, you can have a group named "United States Texas," and disable IM monitoring for that group. Every new agent that is added in the "United States Texas" group automatically gets a configuration with IM monitoring disabled.

You can roll out configuration changes in stages using Agent Groups. In addition, you can create groups for exceptions to monitor particular computers or sets of computers differently. For example, you can create an Executive Staff group for cases when the executive staff is not subject to configurations that apply to the rest of the organization

The ability to change an agent group action is useful when you need to troubleshoot problems in Symantec Data Loss Prevention. For example, you can create a temporary group that disables certain monitoring and configurations for employees (printing with a specific application, for example) to get around a security issue, then change the employees back to the old group when the printing problem is resolved

See "Developing a strategy for deploying Agent Groups" on page 1444.

## Developing a strategy for deploying Agent Groups

Before you begin implementing Agent Groups, think about the agent configurations that you need in your environment. Here's a high-level checklist of planning tasks:

- Identify the unique agent configurations that you need in your environment. Think about all of your agents and how you want them grouped.
- 2. Document who (which agents) gets which configurations.
- 3. Document the Active Directory attributes that you use to create the groups.
- Design the groups so that no user belongs to more than one group. In other words, design groups so that there are no overlapping groups.

See "Overview of the agent group deployment process" on page 1445.

## Overview of the agent group deployment process

Defining and managing user-attribute-based groups involves several tasks and steps, from defining the attributes, creating groups, assigning configurations to deploy the groups, and resolving group conflicts. Table 74-1 provides an overview of the process of deploying agent groups, with cross references to more detailed procedures.

Implementing your Agent Group Strategy **Table 74-1** 

Step	Action	For more information
этер	Action	Tot more information
Step1	Define attributes to use for creating groups.	See "Creating and managing agent attributes" on page 1446.
Step 2	Verify that the attribute definitions are correct using the attribute verification tool.	See "Verifying attribute queries with the Attribute Query Resolver tool" on page 1449.
Step 3	Push attributes to the agents. The agent receives agent attribute queries and the attribute result set is generated and saved on the agent.	See "Applying a new attribute or changed attribute to agents" on page 1450.
Step 4	View the attribute values that are reported by the agents to verify that they return the expected attribute values.	
Step 5	Create the groups you want using the defined attributes.	See "Creating a new agent group" on page 1453.
Step 6	Assign an agent configuration to the group.	See "Assigning configurations to deploy groups" on page 1454.
Step 7	Verify that assignments are correct by confirming that each group contains the expected number of agents.	See "Viewing and managing agent groups" on page 1451.

	27 0 1	,
Step	Action	For more information
Step 8	Periodically check if there are any agent group conflicts. If there are conflicts, resolve them.	See "Viewing group conflicts" on page 1455.

Table 74-1 Implementing your Agent Group Strategy (continued)

See "Migrating pre-12.5 Endpoint deployments to agent groups" on page 1446.

## Migrating pre-12.5 Endpoint deployments to agent groups

Agent Groups is backward-compatible with pre-Symantec Data Loss Prevention 12.5 one server per one-agent configurations. When upgrading from previous releases, the upgrade process automatically creates agent groups for each individual existing Endpoint Server and assigns the configuration associated with that server to the corresponding group during upgrade. The pre-12.5 agents continue to get the same configuration that their Endpoint Server had before upgrade. The upgrade process creates a Default Group, and assigns a Default Configuration.

Note: Default Groups are available for freshly installed Symantec Data Loss Prevention 12.5 endpoints as well, but an administrator can create a new group for the Endpoint Server.

For example, an administrator can add a new Endpoint Server for the Asia - Pacific - Japan region. Since this is a new deployment, and the configuration management strategy is not yet decided, the administrator is not ready to create various agent groups for APJ region. In this case, the administrator can create an endpoint group for the newly added Endpoint Server and assign one configuration that is specific to the APJ region. This enables the administrator to have one unique configuration for all endpoints from the APJ region that are connected to the newly added Endpoint Server for APJ region. Specific groups addressing business needs for this region can be defined later.

See "Creating and managing agent attributes" on page 1446.

## Creating and managing agent attributes

To navigate to the Agent Attributes screen from the System > Agents > Agent Groups screen, click the Manage Agent Attributes link.

Agent Groups are defined using agent attributes. On the **Agent Attributes** screen, you can see a list of predefined and user-defined attributes. Notice that if the list contains only predefined attributes, the Export, Apply Changes, and Undo Changes buttons are not disabled; these actions can only be taken on user-defined attributes.

From this screen you can use the buttons to

- Create new attributes See "Creating a new agent attribute" on page 1448.
- Export attributes See "Verifying attribute queries with the Attribute Query Resolver tool" on page 1449.
- Apply attribute changes. Note that attribute's values are not fetched from Active Directory until you click **Apply** - See "Applying a new attribute or changed attribute to agents" on page 1450.
- Undo attributes changes See "Undoing changes to agent attributes" on page 1451.

Use the **Filters** button to filter the list of attributes by any of the headings.

There are two types of agent attributes, predefined and user-defined. Predefined attributes cannot be deleted or modified. Symantec Data Loss Prevention provides six predefined attributes:

**Table 74-2** Predefined attributes

Attribute	Definition
Agent Host Domain	Domain to which the agent host computer is joined
Logged in User Domain	Current logged-in user domain
Agent Host Name	Computer name of endpoint where the agent is installed
Agent Host Type	Operating system architecture; for example x86 or x64
Agent Host Version	Operating system; for example, Mac OS, Windows 7
Logged in User	Current logged-in user

User-defined attributes are created by the administrator for the purpose of creating groups. You can create user-defined attributes based on Active Directory (AD) attributes. User-defined attributes can be deleted or modified.

Note: User-defined attributes are not supported for computers running Mac OS.

See "Creating a new agent attribute" on page 1448.

#### Creating a new agent attribute

You can create a logical grouping of endpoint agents based on conditions based on user-defined agent attributes. For user-defined attributes, the agent executes an Active Directory query that can resolve the attribute values. When an agent starts up, queries are executed and the attribute results are cached.

To create user-defined attributes, follow these steps:

- 1. Choose **Agent Groups** from the **System > Agents** menu. Then, click the Manage Agent Attributes link.
- 2. On the Agent Attributes screen, click New to begin the attribute creation process.

A Configure Agent Attribute screen appears.

- Add the name of the attribute. Names can contain 1 to 100 characters.
- 4. Add a description of attribute. Descriptions must contain only alpha and numeric characters.
- 5. Select a domain, either User Domain or Machine Domain.

There are two types of attributes for user-defined agent groups:

- User Domain Attributes related to the logged-in user; for example, the domain attribute "department."
- Computer domain Attributes related to the computer; for example, computer attribute "location."
- 6. Add a search filter. You can select from existing applied attributes to define a search filter.

See "Defining a search filter for creating user-defined attributes" on page 1449.

- 7. Specify an Active Directory attribute.
  - Only Active Directory attributes are supported for user-defined agent group attributes.
- 8. Click **Save**. Clicking **Save** saves your attribute but does not apply it.
- 9. Test the attribute and fix any issues you find in testing.

To test, export the attribute(s) from the **Attribute List** screen and review the attribute.

Then, use the Attribute Query Resolver test tool that runs on the Windows host where the endpoint is installed, to test the attribute.

See "Verifying attribute queries with the Attribute Query Resolver tool" on page 1449.

- 10. Apply the tested attributes. Agents start reporting attribute values as soon as the agents resolves the attributes on Active Directory.
- 11. Verify that agents are reporting attribute values. Go to the **System > Agents** > Overview > Agent List screen and verify that the agents are reporting attribute values. You can select a particular agent entry and see the Preview Pane. The Preview Pane lists all predefined and user-defined attributes and their values, conflicts, and alerts.

See "Using the Agent List screen" on page 1460.

See "Defining a search filter for creating user-defined attributes" on page 1449.

#### Defining a search filter for creating user-defined attributes

You can use both Predefined and applied user-defined attributes. The typical syntax for a search filter is

```
(& (objectCategory=Person)
(objectClass=User) (uid=$LoggedinUser$))
```

The value embedded in dollar (\$ \$) signs represents the agent attribute that you can choose when you click the Select from existing attributes drop down on the Configure Agent Attributescreen.

See "Verifying attribute queries with the Attribute Query Resolver tool" on page 1449.

#### Verifying attribute gueries with the Attribute Query Resolver tool

You can verify if the attribute definitions are correct with the Attribute Query Resolver tool. First, export the attributes to an XML file:

- 1. Go to the System > Agents > Agent Groups > Agent Attributes screen.
- 2. Click **Export** to export the attributes data to an XML file.
- 3. Click Save File in the Opening agent-attributes.xml dialog.
- 4. Click **OK** to complete the export task.

Next, use this XML file to test your attributes with the Attribute Query Resolver tool.

Note: You must have administrator privileges to run this tool.

- 1. Copy AttributeQueryResolver.exe and aqp.dll from the agent distributable tools folder on the endpoint into the same folder.
- 2. Run the command (for example)

```
c:\AttributeQueryResolver.exe -aq=agent-attributes.xml
```

3. Attributes with errors display in the output with blank values. For example, if the attribute User Email had an error, it displays as User Email= with no value. Errors can occur if a user provides an incorrect search filter, if a specified attribute does not exist in Active Directory, or if Active Directory is not reachable.

You can go to the AttributeQueryResolver.log log file to view details for the attribute errors. In this attribute error log, files with no errors display an Error code: 0 (no errors). Attributes with errors display an error code and error description. For example, the User Email attribute with a blank attribute in the output (indicating an error) displays an error message that reads:

```
2014-01-21 20:41:48 | AttributeQueryResolver | SEVERE | Attribute
: User Email Error code: -2147463161 Error description :
E ADS PROPERTY INVALID
```

If you provide an invalid XML file as a parameter to the Attribute Query Resolver tool, or if you do not have appropriate rights to run the tool, the following SEVERE error is logged:

```
AttributeQueryResolver | SEVERE | Query store is not open.
```

If the attribute definitions are correct, you can deploy the attributes to agents. If there are errors, edit the attributes reporting errors, export the attributes, and run them through the Attribute Query Resolver tool. Repeat this process until there are no errors.

See "Applying a new attribute or changed attribute to agents" on page 1450.

#### Applying a new attribute or changed attribute to agents

Newly created agent attributes appear on the Agent Attributes screen labeled as New. After you edit an agent attribute, the attribute is in a Modified state. In both cases, you must apply the attributes to the agents before they can take effect. To apply the changes to the agents:

- Click Apply Changes on the Agent Attributes page.
- 2. Verify the changes that appear on the Apply Changes pop-up and click Apply Changes. If you see any discrepancies, click Cancel and go back to previous screens to correct your errors.
- 3. Review the updated **Agent Attributes** screen. The **Status** of your recently applied agent attributes should now read Up-to-date.

See "Undoing changes to agent attributes" on page 1451.

#### Undoing changes to agent attributes

After you have modified certain attributes and tested them with the Attribute Query Resolver tool, you may find issues with the modified attributes. You can undo changes to go back to the original state of the attributes. To undo changes, follow these steps:

- 1. Click Undo Changes.
- 2. In the **Undo Changes** dialog, review the list of changed attributes.
- Click Undo Changes to reverse the most recent changes you made.

See "Editing user-defined agent attributes" on page 1451.

#### Editing user-defined agent attributes

You can edit user-defined agent attributes from the System > Agent > >Agent Groups > Agent Attributes screen:

- 1. Click the attribute in the Name column. User-defined attributes are all of the Type User Defined.
- 2. Edit the attribute fields on the System > Agents > Agent Groups > Edit Agent Attribute screen.
- Click Save.

Note: You cannot edit Predefined agent attributes.

See "Viewing and managing agent groups" on page 1451.

## Viewing and managing agent groups

You can use agent groups to enable logical grouping of your endpoint computers based on conditions. Agent groups can be based on

- Agent attributes
- **Endpoint Server names**
- **Endpoint host names**

Agents are evaluated and included in particular groups based on a priority ordering of conditions. The conditions are, from highest priority to lowest:

- 1. An agent host name that is in the "Always include" list in the agent group definition.
- 2. An agent that connects to an Endpoint Server group, when a corresponding Endpoint Server group exists.
- 3. An agent group with a user-defined attribute, where the agent satisfies its group condition.

For example, if an agent can belong to both the "Endpoint host name group" and the "Agent attribute" based group, since the Endpoint host name group has highest priority among all three types of groups, the agent belongs to Endpoint host name group.

Check agent group status and manage agent groups from the **System > Agents** > Agent Groups screen. To view agent group conflicts, click View Agent Group **Conflicts** on the right-hand side of the screen.

Information about agent groups is divided into several columns on this page. You can click any column header to sort entries alphanumerically in that column. Click the column header again to sort in reverse order.

Use these buttons to perform the following actions:

- New Create a new agent group.
- **Delete** Delete the selected agent groups.
- Enable Enable the selected agent groups.
- **Disable** Disable the selected agent groups.
- Assign Configuration Assign a configuration to created or updated agent groups.
- Update Configuration Update a configuration for the selected agent groups.
- Filters Reorganize this list of agent groups for easier viewing.

See "About agent groups" on page 1443.

See "Overview of the agent group deployment process" on page 1445.

See "Agent group conditions" on page 1452.

## Agent group conditions

An agent group definition can have multiple conditions. In addition, the following operators are supported for group conditions:

- Implicit AND conditions
- OR is supported for a condition by specifying multiple values for the condition

- Equal TO clause
- Wildcard character (\*) to specify multiple values. For example, "Fin\*" matches both "Finance" and "Fincon"

You can navigate to the main **Agent Groups** screen in the Enforce Server administration console at System > Agents > Agent Groups.

See "Creating a new agent group" on page 1453.

#### Creating a new agent group

To create an agent group:

- Go to the System > Agents > Agent Groups screen.
- 2. Click New to create a new group. This action takes you to the Create New Agent Group screen.
- 3. Enter the name of the group in the **Name** field. The name is a required field and must contain from 1 to 100 characters.
- 4. Add an optional description.
- 5. Click a button to define the group condition as either **User Attributes** or **Endpoint Server.**
- 6. Select attributes for the condition from the Select Agent Attributes list and assign values to match, to create the condition.
- 7. Add agent host names to the Always include these agents box if you have agents that you want to always include in this group.
- 8. Click **Save** when you are done, or **Cancel** to start over.
- 9. Assign the configuration to deploy the group. See "Assigning configurations to deploy groups" on page 1454.

Note: Assigning a configuration to the group activates the group.

See "Overview of the agent group deployment process" on page 1445.

See "Assigning configurations to deploy groups" on page 1454.

#### Updating outdated agent configurations

When an agent configuration is updated, but before the changes have been applied to an agent group, the agent group has an outdated configuration. Outdated agent configurations appear in the System > Agents > Agent Groups list with their name flagged with a red exclamation mark. To update an outdated group configuration:

- Choose an agent group to update the configuration on the System > Agents > Agent Groups screen.
- 2. Click the check box for the agent group with the outdated configuration you want to update.
- 3. Click Update Configurations.
- 4. Verify the name and status for the group in the **Update Configurations** dialog and click OK.
- 5. Verify that each configuration for the group has been updated by assuring that there is no longer a red exclamation mark following the names of the agent configurations.

Note: If an agent is offline, it does not receive an updated configuration until the agent comes online again.

See "Verify that group assignments are correct" on page 1454.

## Assigning configurations to deploy groups

To deploy created or updated groups, you need to assign configurations to the groups. To assign a configuration to a group or set of groups:

- 1. Select the groups on the **System > Agents > Agent Groups** screen by clicking the check boxes to the left of each group.
- 2. Click **Assign Configuration** in the action bar.
- 3. Choose a configuration from the **Assign Configuration** dialog.
- 4. Click **OK** in the **Assign Configuration** dialog box.
- 5. When the Agent Groups page refreshes, the Assigned Configuration names are displayed for the groups.

See "Updating outdated agent configurations" on page 1453.

## Verify that group assignments are correct

Confirm that you have the expected number of agents in each of the groups:

- 1. Go to System > Agents> Overview > Summary Reports.
- 2. Click Advanced Filters & Summarization and choose Summarize By : Agent
- 3. Verify that you have the expected number of agents reporting in each of the groups.

See "Viewing group conflicts" on page 1455.

## Viewing group conflicts

As the Endpoint administrator, you determine the correct agent group for each endpoint computer based on the attribute values that the agent on the endpoint reports to the Endpoint Server. You can avoid group conflicts by carefully planning your implementation. You should also periodically check to see if there are group conflicts.

You can see conflicts on the View Conflicts screen by clicking View Agent Group Conflicts link on the System > Agents > Agent Groups screen. On the View Conflicts screen, under the Conflicting Groups heading, you see the names of the conflicting groups.

If a particular agent can qualify to be a part of more than one group, a conflict arises. For simple conflicts, where group 2 is a subset of group 1, Symantec Data Loss Prevention automatically resolves the conflict in favor of the subset group 2. For example, if you have these two groups:

- Group US={Country=US}
- Group Texas={Country=US & State=Texas}

the conflict between group "US" and group "Texas" is resolved to group "Texas" because group "Texas" is a subset of group "US."

No automatic group conflict resolution mechanism exists for non-subset groups that are in conflict. For example, if you have a group called US HR in which the Country=US and the Department=HR, and a Group US VP in which the Country=US and the Designation=VP, agents that belong to VPs in the HR department will result in a conflict. Since Department=HR is not a subset of Designation=VP (or vice versa), the conflict cannot be resolved and the agents with conflicts are placed in a warning state and continue to belong to whatever group they belonged to before the conflict arose. For these more complex conflicts, Symantec Data Loss Prevention reports conflicts and you must edit the group definitions to resolve the group conflicts.

See "Changing groups" on page 1455.

## Changing groups

You can change groups for agents to have a different configuration on the System > Agents > Agent Groups > Agent List screen. The ability to change an agent configuration from one group to another is useful in many situations, especially when you need to troubleshoot a problem with Symantec Data Loss Prevention.

For example, say that your employees in the group Trading Group Texas have problems printing with the stock trading application. This issue causes a major problem for your business, as traders are not able to work without the ability to print. You can move the agents in Trading Group Texas to a temporary group, called Troubleshoot Trading Group, with print monitoring disabled, until you can troubleshoot the agent endpoints and fix the issue. After the problem is solved, you can change the group back to Trading Group Texas to enable print monitoring.

To change groups for agent configurations:

- Click the checkboxes for the agent entries that you want to move.
- 2. Click Change Group.
- 3. Choose a new group from the System > Agents > Agent List > Agent Group menu.
- 4. Click OK.

See "About Symantec DLP Agent administration" on page 1457.

# Managing Symantec DLP Agents

This chapter includes the following topics:

- About Symantec DLP Agent administration
- About Endpoint Agent logs

## About Symantec DLP Agent administration

After you have installed Symantec DLP Agents, you can administer them from the Enforce Server. The Enforce Server provides an interface which can be used to:

- View Symantec DLP Agent information.
- View the status of your deployed Symantec DLP Agents.
- View events for Symantec DLP Agents.
- Generate reports for your deployed Symantec DLP Agents.
- Troubleshoot your deployed Symantec DLP Agents.

To view and manage your Symantec DLP Agents, log on to your Symantec Data Loss Prevention Enforce Server; then, click **System > Agents**.

See "Agent Overview screen" on page 1457.

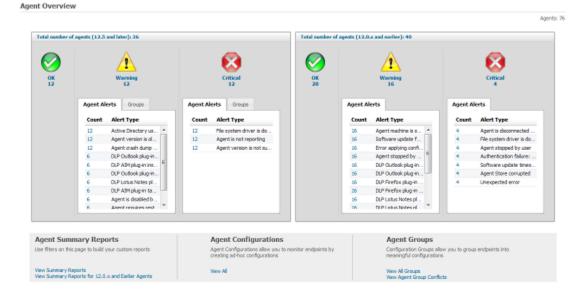
See "Agent events" on page 1490.

#### Agent Overview screen

The **Agent Overview** screen provides a summarized view of all deployed DLP Agents. You can use this screen to view the DLP Agent health status and to begin troubleshooting any agents which might report an alert. The DLP Agents are grouped

by status and then they are categorized by alert type. Alert types with the highest number of affected agents are listed first and alert types with the fewest number of affected agents are listed last.

Figure 75-1 Agent Health Dashboard



You can begin troubleshooting an alert by clicking a status icon or by clicking on a link to the left of an alert type. After you click a status icon or link the Agent List screen displays. See "Using the Agent List screen" on page 1460.

The DLP Agents are grouped into the following statuses:

**Table 75-1 DLP Agent statuses** 

DLP Agent status	Status description
	An <b>OK</b> status indicates that the DLP Agents in this state are operating under normal conditions. This status indicates:
ок	<ul> <li>Services and the file-system drivers for the DLP Agent are running</li> <li>The DLP Agent cache is created and available</li> <li>The DLP Agent is reporting to the Endpoint Server as expected</li> </ul>

DLP Agent statuses (continued) Table 75-1

DLP Agent status	Status description
A	A <b>Warning</b> status indicates that the DLP Agents in this state have experienced conditions which may require attention.
Warning	Warning agent alerts generally include the following:  Downlevel DLP Agent version  Active Directory group resolution failure  A plug-in error has occurred  The DLP Agent needs to be restarted  The following section provides a comprehensive list of Warning statuses.  See "Troubleshooting agent alerts" on page 1493.
Critical	A Critical status indicates that the DLP Agents in this state have experienced conditions that require immediate attention:  Critical agent alerts generally include the following:  A driver is not running  The DLP Agent version is not compatible with the Endpoint Server  Active Directory permissions conflict with Symantec Data Loss Prevention permissions.  The DLP Agent cannot report to the Endpoint Server  The following section provides a comprehensive list of Critical statuses.  See "Troubleshooting agent alerts" on page 1493.

The Agent Overview screen lets you quickly access agent summary reports, agent configurations, and agent groups.

Table 75-2 Agent management features

Section	Description	
Agent Summary Reports	Agent summary reports let you summarize agent information and create reports.	
	See "Using the Summary Reports screen" on page 1467.	
	See "Using the Summary Reports for 12.0.x and Earlier Agents screen" on page 1473.	
Agent Configurations	You can configure agent settings on the <b>Agent Configurations</b> screen.	
	See "About agent configurations" on page 1405.	

Table 75-2	Agent management features	(continued)
Tubic / J Z	Agent management reature.	(continuca)

Section	Description
Agent Groups	You can view existing agent groups and resolve agent group conflicts.
	See "About agent groups" on page 1443.
	See "Viewing group conflicts" on page 1455.

See "Using the Agent List screen" on page 1460.

See "Agent events" on page 1490.

#### **Using the Agent List screen**

You access the Agents List screen by clicking an agent status or alert type link on the System > Agents > Overview screen. The Agents List screen helps you manage agents by displaying agent details and status. You can also use this screen to modify agents.

See "About agent status" on page 1463.

You use the Summary Reports for 12.0.x and Earlier Agents screen to manage and troubleshoot 12.0.x and earlier agents. See "12.0.x and earlier agent actions" on page 1485.

You can use the **Agents List** screen to perform agent management tasks.

Note: Use the **Filters** feature to execute or remove filters you select. See "Agent filtering" on page 1466.

#### Agent management tasks **Table 75-3**

Agent management task	Description
Troubleshoot	This menu lets you perform the following troubleshooting tasks:
	<ul> <li>Enable         Enables the disabled agents.         Enabled agents automatically reconnect with the         Endpoint Server and obtain the most current policies.         Enabling an agent enables monitoring on that endpoint.         Enabled agents can log events on the Endpoint Server.</li> <li>Disable         Stops monitoring and any active scans on agents.</li> <li>Set Log Level         Sets the logging level for the specified agent. Symantec Technical Support uses agent logs for troubleshooting purposes.</li> </ul>
	Note: It is recommended to contact Symantec Technical Support before you change the log level for an agent.
	<ul> <li>Reset Log Level         Resets the logging level for the specified agent to the default INFO level. Symantec Technical Support uses agent logs for troubleshooting purposes.         See "About Endpoint Agent logs" on page 1500.</li> <li>Set Under Investigation         Set if you believe there is some sort of issue with the agent. You can set this status regardless of whether the agent is running, disabled, or shut down. An additional icon, a flag, appears next to the main status icon of the agent.</li> <li>Remove Under Investigation         Remove Under Investigation status from the selected agents.</li> </ul>
	Note: These troubleshooting tasks are also available on the 12.0.x and earlier Summary Reports screen. When you click on an agent on the Agent List screen, detailed information displays in the preview pane. This pane provides additional detail on the agent reporting status.

Agent management tasks (continued) Table 75-3

Agent management task	Description
Delete	Deletes the agent.
	When you delete an agent, you remove that agent and all associated events from the Endpoint Server. It is no longer visible in the Enforce Server administration console. Deleting an agent from the Endpoint Server does not mean that it has been uninstalled from the endpoint.
Change Server	Lets you change the Endpoint Server to which the agent connects.
	You can specify the primary Endpoint Server as well as secondary Endpoint Servers in case the primary server fails and the agent must switch connections.
	See "Changing the Endpoint Prevent Server" on page 1490.
Change Group	Lets you assign the selected agent to an agent group that you select.
	See "Agent task confirmation screen" on page 1487.
Restart	Restarts the selected agent.
Shut Down	Shuts down the selected agent.
	Note: For version 12.5 agents, the Agent Shutdown by service tool event no longer displays on the Agent Events screen (Systems > Agents > Events). However, this event displays for 12.0.x and earlier agents.
	See "Agent events" on page 1490.

Table 75-3	Agent man	agement tasks	(continued)
lable / 5-5	Agent man	iageillelli tasks	(continued)

Agent management task	Description
Pull Logs	Lets you pull agent logs and operational logs for the agent. You can pull either the agent logs, or the operational logs, or both sets of logs.
	Pulling agent logs is a two-step process:
	<ul> <li>Click the Pull Logs button to download the agent logs from the endpoint to the Endpoint Server.</li> <li>Download the agent logs from the Endpoint Server through the Enforce Server. You complete this action on the System &gt; Servers &gt; Logs &gt; Collection screen.</li> </ul>
	See "Collecting server logs and configuration files" on page 257.
	When the logs are pulled from the endpoint, they are stored on the Endpoint Server in an unencrypted format. After you collect the logs from the Endpoint Server, the logs are deleted from the Endpoint Server and are stored only on the Enforce Server. You can only collect logs from one endpoint at a time.

See "Agent Overview screen" on page 1457.

See "About filters and summary options for reports" on page 1046.

See "Agent events" on page 1490.

See "Using the Summary Reports screen" on page 1467.

#### About agent status

The Agent List screen displays current agent information. You can use this information to review agent status, last update time, agent operating system, and version. Table 75-4 provides a list of agent statuses and details.

Table 75-4	Agent status
Section	Description
Status	Displays the current agent status.  Agent status includes the following:  OK  Indicates the agent service and file-system driver are running, that the cache is created and available, and that the connection functions as expected.  Warning  Indicates the agent may need attention. For example, Symantec Data Loss Prevention assigns this status when the endpoint data share nears its storage limit.
	Indicates that the agent is experiencing transitory connection problems. The agent may have been down for a period of time. Policy and configuration may be out of date. The agent may not be compatible with the Enforce Server.  Investigating Indicates that the agent in question is under investigation. Agents may be under investigation for a number of reasons. These reasons include sending too many false positive incidents, and being unable to connect to the Endpoint Server.  Not Investigating You select this item to remove an agent from investigation.  Log Level Changed Indicates that the log level for the agent has been changed or reset. See "About Endpoint Agent logs" on page 1500.  Default Log Level You select this item to change the log level. See "About Endpoint Agent logs" on page 1500.
Alerts	Displays the number of Warning and Critical alerts that occur on an agent. To see a list of alerts for a particular agent, click on the relevant agent entry to display the <b>Events</b> screen.  See "Agent events" on page 1490.
Machine Name	Displays the endpoint name.
Agent Group	Displays the agent group name.

Table 75-4Agent status (continued)

Section	Description
Agent Configuration	Displays the current agent configuration used:  Other Configurations (Not Current) Indicates that a custom configuration is applied.  Current Configuration Indicates that the latest configuration is applied.  Outdated Configuration Indicates that the configuration is obsolete.  Unknown/Deleted Configuration Indicates that the configuration was deleted. Agents display this configuration status until they receive an updated configuration from an Endpoint Server.  Default Configuration Indicates that the default configuration is applied. The default configuration is applied during install.
Connection Status	Displays the current agent connection status.  Agent connection status includes the following:  Unknown Agents with unknown status.  Reporting DLP Agents that are currently connected to the corporate network.  Not Reporting DLP Agents that are not currently connected to the corporate network.  See "Setting the endpoint location" on page 1378.
Last Update Time	Displays the date and time on the Enforce Server when the agent was last updated.
os	Displays the agent operating system.
Platform	Displays the agent processor type.
Endpoint Server	Lists the Endpoint Server to which the agent is registered.
IP Address	Displays the endpoint IP address.
Version	Displays the endpoint version.

See "Agent Overview screen" on page 1457.

See "About filters and summary options for reports" on page 1046.

#### Agent filtering

You can filter what agents display on the Agent List screen by clicking Filters. After you are done selecting filter criteria, click the check box.

Note: You filter 12.0.x and earlier agents on the Summary Reports for 12.0.x and Earlier Agents screen. See "Using the Summary Reports for 12.0.x and Earlier Agents screen" on page 1473.

Click a column header to sort entries alpha-numerically. Click the column header a second time to sort in reverse order. By default, Symantec Data Loss Prevention lists agents by the endpoint name. Select items in the column headers to only display agents containing the selected data.

You can filter the agents that display by a number of criteria including agent configuration, server name, and agent IP address. Additionally, you can filter the agent events by specific sets of criteria relating to the Symantec DLP Agent. Summarizing and filtering the agents lets you view agents by specific criteria, and in the order that you want. For example, you can display the agents that have the Default Configuration associated and then display the agents that were updated in the last 7 days. You can click a column to the agents by the date they were last updated.

Note: Click Select all to select all agents that meet the filter criteria regardless of what agents currently display on the grid. This selection is useful when agents flow across more than one page. Click the box at the top left of the grid to select all agents that display on the grid.

You can filter the agents that display in the grid by using the following items:

**Table 75-5** Filtering agents

Item to filter	Description	
Alert Category	Lets you filter on each of the agent alert categories.	
Status	Select an agent alert status.	
Machine Name	Enter the name of an endpoint you want to display. The alphanumeric value you enter displays all endpoints that contain the value string. For example, to display endpoints with 123 anywhere in the name, enter 123.	
Agent Group	Select an agent group to display all the agents that are contained in the group.	

Item to filter	Description	
Agent Configuration	Select an agent configuration.	
Connection Status	Select a connection status.	
Last Update Time	Select an update time. This value represents the last time the Enforce Server received data from agent.	
os	Enter the name of the OS you want to display. The alphanumeric value you enter displays all endpoints that contain the value string. For example, to display endpoints with Mac anywhere in the name, enter Mac.	
Platform	Select 32bit or 64bit.	
Endpoint Server	Click the Endpoint Server name to display the agent associated with that server. You can also select <b>Deleted</b> to display agents currently reporting to deleted Endpoint Servers.	
IP Address	Enter an IP address associated with an agent.	
Version	Enter the agent version you want to display.	

Filtering agents (continued) **Table 75-5** 

See "Using the Agent List screen" on page 1460.

#### **Using the Summary Reports screen**

You use the Summary Reports screen (System > Agents > Overview > Summary > Reports) to summarize agent information and create reports.

Note: You complete agent management tasks on the Agent List screen. See "Using the Agent List screen" on page 1460.

You can select which DLP Agents display in a report by filtering the agent events by specific sets of criteria. For example, you can summarize the agents by the associated agent configuration and then filter those configurations by the most recently updated agents.

You can generate a filtered report by specifying a number of criteria, including agent configuration, server name, and agent IP address. Summary reports take their name from the summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

#### To create a DLP Agent summary report:

- 1 Click Advanced Filters and Summarization.
- 2 Select an item in the Summarize By list to select on which criteria you want to summarize.

See Table 75-6 on page 1468.

You can summarize by the following items:

- Agent Configuration
- Agent Group
- Agent IP
- Agent Status
- Agent Version
- Alerts
- Connection Status
- **Endpoint Server**
- **Investigating State**
- Last Connection Time
- OS
- Platform
- State Category
- State Sub Category
- 3 Click Add filter if you want to add additional filters. Table 75-6 lists advanced filters.
- 4 Click **Apply** to generate the report using the specified filters.
- 5 Click **Save > Save As** to save the report you created.
- 6 Click **Send** to email the report.
- 7 Click **Export > All: CSV** to download a CSV file of the report.

Advanced filters and summarization **Table 75-6** 

Primary filter	Available conditions	Secondary filter
Agent Configuration	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	Agent Configuration: Select the DLP Agent Configuration that you want to include or exclude from the report.

Advanced filters and summarization (continued) **Table 75-6** 

Primary filter	Available conditions	Secondary filter
Agent Configuration Status	■ Is Any Of ■ Is None Of	<ul> <li>Current Configuration: The number of agents that are running the most current version of the agent configuration.</li> <li>Outdated Configuration: The number of agents that are running an older version of the agent configuration.</li> <li>Unknown/deleted Configuration: The number of agents that are running an unknown version of the agent configuration.</li> </ul>
Agent Group	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	Select an agent group from the list.
Agent Group Status	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	<ul> <li>Deleted: The agent groups that have been deleted.</li> <li>Disabled: The agent groups that have been disabled.</li> <li>Enabled: The agent groups currently in use.</li> </ul>
Agent IP	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts With</li> <li>Ends with</li> </ul>	Agent IP: Enter the IP address you want to filter.
Agent Status	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	<ul> <li>Critical: Filter DLP Agents which report a Critical status.</li> <li>OK: Filter DLP Agents which report an OK status.</li> <li>Warning: Filter DLP Agents which report a Warning status.</li> </ul>

Advanced filters and summarization (continued) **Table 75-6** 

Primary filter	Available conditions	Secondary filter
Agent Version	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts With</li> <li>Ends With</li> </ul>	Agent Version: Enter the DLP Agent version number which you want filtered.
Alerts	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	Alerts: Enter the DLP Agent alert you want filtered.
Connection Status	■ Is Any Of ■ Is None Of	<ul> <li>Not Reporting: Filter DLP Agents that are not currently connected to the corporate network.</li> <li>Reporting: Filter DLP Agents that are currently connected to the corporate network.</li> <li>Unknown: Filter DLP Agents that have an unknown connection status.</li> </ul>
Endpoint Server	■ Is Any Of ■ Is None Of	Endpoint Prevent Server: Select the Endpoint Prevent Server you want to filter. The DLP Agents that report to this server are filtered.  Selecting Deleted displays all endpoints that report to deleted Endpoint Servers.
Investigating State	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	<ul><li>Investigating</li><li>Not Investigating</li></ul>
Log Level	■ Is Any Of ■ Is None Of	<ul> <li>Custom: Select all DLP Agents with log levels set to a value other than the INFO level.</li> <li>Default: Select all DLP Agents with log levels set to the default INFO level.</li> </ul>

Advanced filters and summarization (continued) **Table 75-6** 

Primary filter	Available conditions	Secondary filter
Machine Name	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts with</li> <li>End with</li> </ul>	Machine name: Enter the computer name that you want to use as a filter.
OS	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts with</li> <li>End with</li> </ul>	OS: Enter the operating system name that you want to use as a filter.
Platform	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	<ul><li>32-bit</li><li>64-bit</li></ul>
State Category	■ Is Any Of ■ Is None Of	<ul> <li>AD User Group Resolution</li> <li>Agent Configuration Change Status</li> <li>Agent Group Change Status</li> <li>Agent Monitoring Status</li> <li>AIM Plugin Status</li> <li>Crash Dump Status</li> <li>File System Drive</li> <li>Lotus Notes Plugin Status</li> <li>Outlook Plugin Status</li> <li>Reporting Status</li> <li>Software Compatability</li> </ul>

Advanced filters and summarization (continued) **Table 75-6** 

Primary filter	Available conditions	Secondary filter
State Sub Category		<ul> <li>AD User Group Resolution: Filter DLP Agent by successful or failed Active Directory Group resolution.</li> <li>Agent Configuration Change Status: Filter DLP Agent by date the agent configuration was last updated.</li> <li>Agent Group Change Status: Filter DLP Agent by date the agent group was last updated.</li> <li>Agent Monitoring Status: Filter DLP Agents by their monitored status.</li> <li>AIM Plugin Status: Filter DLP Agents which have AOL Instant Messenger plug-ins that have failed installation, been repaired, or tampered with.</li> <li>Crash Dump Status: Filter DLP Agents that have crash dumps available or DLP Agents that do not have a crash dump.</li> <li>File System Driver: Filter DLP Agents using the status of the file system drivers on the agents.</li> <li>Lotus Notes Plugin Status: Filter DLP Agents which have Lotus Notes plug-ins that have failed installation, been repaired, or tampered with.</li> <li>Outlook Plugin Status: Filter DLP Agents which have Microsoft Outlook plug-ins that have failed installation, been repaired, or tampered with.</li> <li>Reporting Status: Filter DLP Agents that are either reporting or not.</li> <li>Software Compatability: Filter DLP Agents that are either reporting or not.</li> <li>Software Compatability: Filter DLP Agents according to their compatability with Endpoint Servers.</li> </ul>

Summary reports take their name from the summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

Table 75-7describes the columns that display in the summary report you create.

Summary Reports details Table 75-7

Item	Description	
Summary criterion	Identifies the items on which the report summarizes.	
Total	Lists the total number of agents that are associated with the summary criteria.	
Connection Status	Lists the number of agents currently connected to the network.	
Health Status	Lists the number of agents that are marked with an <b>OK</b> , <b>Warning</b> , or <b>Critical</b> health status.	
Configuration Status	Lists the number of agents that are running a current, outdated, or unknown version of the agent configuration.	

See "Agent Overview screen" on page 1457.

See "Using the Agent List screen" on page 1460.

See "About agent configurations" on page 1405.

See "Agent events" on page 1490.

#### Using the Summary Reports for 12.0.x and Earlier Agents screen

The Summary Reports for 12.0.x and Earlier Agents screen provides an overview of the state of your DLP Agents and lets you administer the agents. The statuses are described by individual icons displayed next to each agent. You can also perform agent tasks on any selected agents. Use the check boxes to select the agents that you want to modify.

You can filter the agent events by specific sets of criteria relating to the Symantec DLP Agent. Summarizing and filtering the agents lets you view the agent data in the order that you want. For example, you can summarize the agents by the associated agent configuration and then filter those configurations by the most recently updated agents.

#### To create a filtered DLP Agent summary report:

- 1 Click Advanced Filters and Summarization.
- 2 Select the criteria that you want to filter for by selecting your criteria from the pull-down menus.
  - See Table 75-8 on page 1474.
- If you want to add additional filters, click Add filter. 3
- 4 After you have completed configuring the filters that you want to use for your report, click **Apply** to generate the report.

Advanced filters for DLP Agent summary reports **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Agent Configuration	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	Agent Configuration: Select the DLP Agent Configuration that you want to include or exclude from the report.
Agent Configuration Status	■ Is Any Of ■ Is None Of	<ul> <li>Current Configuration:         The number of agents that are running the most current version of the agent configuration.     </li> <li>Outdated Configuration:         The number of agents that are running an older version of the agent configuration.     </li> </ul>
		■ Unknown/delete Configuration: The number of agents that are running an unknown version of the agent configuration.

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Agent IP	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts With</li> <li>Ends with</li> </ul>	IP address: Enter the IP address or multiple IP addresses to filter.
Agent Status	■ Is Any Of ■ Is None Of	<ul> <li>Disabled: Filter DLP         Agents which report a         Disabled status.</li> <li>Down: Filter DLP Agents         which report a Down         status.</li> <li>Healthy: Filter DLP         Agents which report a         Healthy (OK) status.</li> <li>Shut Down: Filter DLP         Agents which report a         shutdown status.</li> <li>Warning: Filter DLP         Agents which report a         shutdown status.</li> </ul>
Agent Version	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts With</li> <li>Ends With</li> </ul>	Version: Enter the DLP Agent version number which you want filtered.

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Category	■ Is Any Of ■ Is None Of	You can select one the following categories to add to your filter:  AD User Group Resolution Agent Configuration Change Status Agent Group Attribute Discovery Status Agent Group Change Status Agent Group Conflict Status Agent Logger Status Agent Monitoring Status Agent Store Agent Store Agent Troubleshooting Status AIM Plugin Status Configuration Update Connection Status Crash Dump Status Crash Dump Status Pile System Driver Firefox Plugin Status Lotus Notes Plugin Status Outlook Plugin Status Software Compatibility Software Update

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Connection Status	<ul><li>Is Any Of</li><li>Is None Of</li></ul>	Off the Corporate     Network: Filter DLP     Agents that are not     currently connected to the     corporate network.      On the Corporate     Network: Filter DLP     Agents that are currently     connected to the     corporate network.
Endpoint Server	■ Is Any Of ■ Is None Of	Select the Endpoint Prevent Server you want to filter. The DLP Agents that report to this server will be filtered.
Investigating State	■ Is Any Of ■ Is None Of	You can filter DLP Agents by the following investigative states:  Investigating  Not Investigating

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Last Connection Time		You can filter DLP Agents by their last connection time using the following points in time:  Today Yesterday Current Week to Date Current Month to Date Current Quarter to Date Current Year to Date Last 7 Days Last 30 Days Last Week Last Month Last Quarter Custom: Select a date range to filter DLP Agents which have not connected to the Endpoint Prevent Server during the specified date range. Custom Since: Select a date to filter DLP Agents which have not connected to the Endpoint Prevent Server after the specified date. Custom Before: Select a date to filter DLP Agents which last connected to the Endpoint Prevent Server after the specified date. Custom Before: Select a date to filter DLP Agents which last connected to the Endpoint Prevent Server after the specified date.

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Log Level	■ Is Any Of ■ Is None Of	<ul> <li>Custom: Select all DLP         Agents with log levels set         to a higher level than the         INFO level.</li> <li>Default: Select all DLP         Agents with log levels set         to the default INFO level.</li> </ul>
Machine Name	<ul> <li>Contains Ignore Case</li> <li>Does Not Contain Ignore Case</li> <li>Matches Exactly</li> <li>Does Not Match Exactly</li> <li>Matches Exactly Ignore Case</li> <li>Starts with</li> <li>End with</li> </ul>	Machine name: Enter the computer name that you want to use as a filter.

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
Sub Category	■ Is Any Of ■ Is None Of	

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
		■ AD User Group Resolution: Filter DLP Agent by successful or failed Active Directory Group resolution. ■ Agent Logger Status: Filter DLP Agents which have an updated log leve status. ■ Agent Monitoring Status: Filter DLP Agents by their monitored status: Filter DLP Agents by the state of the agent. ■ Agent Store: Filter DLP Agents by the state of the Agent Store. ■ Agent Troubleshooting Status: Filter DLP Agents based on the state of the last attempted task that was executed for the Agent. ■ AIM Plugin Status: Filte DLP Agents which have AOL Instant Messenger plug-ins that have failed installation, been repaired or tampered with. ■ Configuration Update: Filter DLP Agents that have encountered an erro or have successfully updated the agent configuration. ■ Connection Status: Filte DLP Agents that have encountered authentication failures, have an active connection, have a closed

Advanced filters for DLP Agent summary reports (continued) **Table 75-8** 

Primary filter	Available conditions	Secondary filter
		connection, or lost connection to the Endpoint Prevent Server.  Crash Dump Status: Filter DLP Agents that have crash dumps available or DLP Agents that do not have a crash dump.  Detection: Filter DLP
		Agents that have a full detection queue, have experienced a detection timeout, or have had files removed from the Agent Store.
		■ File System Driver: Filter DLP Agents using the status of the file system drivers on the agents.
		■ Firefox Plugin Status: Filter DLP Agents which have Firefox plug-ins that have failed installation, been repaired, or tampered with.
		Lotus Notes Plugin Status: Filter DLP Agents which have Lotus Notes plug-ins that have failed installation, been repaired or tampered with.
		■ Outlook Plugin Status: Filter DLP Agents which have Microsoft Outlook plug-ins that have failed installation, been repaired or tampered with.
		Software Compatibility     Filter DLP Agents by thei     compatibility with the     Endpoint Prevent Server

**Table 75-8** Advanced filters for DLP Agent summary reports (continued)

Primary filter	Available conditions	Secondary filter
		■ Software Update: Filter DLP Agents that are being updated by the status of each attempted update.

You can generate a summarized report by specifying a number of criteria including agent configuration, server name, and agent IP address. View the summary criteria available by clicking the Advanced Filters and Summarization link and then clicking the **Summarize By** drop-down menu. The administration console displays all criteria in alphabetical order. Select the criteria you want from the summarize field and then click **Apply**. Summary reports take their name from the summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

#### To create a summarized DLP Agent summary report:

- Click Advanced Filters and Summarization. 1
- 2 Locate the **Summarize By** pull-down menu; then, select the type of summarized report you want to view.
- 3 Click **Apply** to create the report.

Note: Summary reports take their name from the summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

**Table 75-9** Summary Reports screen details

Item	Description	
Summary criterion	Lists the summary items. The available summary criteria are the following:	
	<ul> <li>Agent Configuration</li> <li>Agent Configuration Status</li> <li>Agent IP</li> <li>Agent Status</li> <li>Agent Version</li> <li>Category</li> <li>Connection Status</li> <li>Endpoint Server</li> <li>Investigating State</li> <li>Last Connection Time</li> <li>Log Level</li> <li>Machine Name</li> <li>Sub Category</li> </ul>	
Total	The total number of agents that are associated with the summary criteria.	
Connected	The number of agents currently connected to the network.	
Disconnected	The number of agents currently disconnected from the network.	
Healthy	The number of agents that are marked with a <b>Healthy</b> status.	
Warning	The number of agents that are marked with a <b>Warning</b> status.	
Down	The number of agents that are marked with a <b>Down</b> status.	
Disabled	The number of disabled agents.	
Shut Down	The number of agents that have been shut down.	
On Current Configuration	The number of agents that are running the most current version of the agent configuration.	

Item	Description
Outdated	The number of agents that are running an older version of the agent configuration.
On Unknown	The number of agents that are running an unknown version of the agent configuration.

**Table 75-9** Summary Reports screen details (continued)

See "Agent Overview screen" on page 1457.

See "Using the Agent List screen" on page 1460.

See "Using the Summary Reports screen" on page 1467.

See "About agent configurations" on page 1405.

See "Agent events" on page 1490.

## 12.0.x and earlier agent actions

The following table describes the available agent actions that you can take on 12.0.x and earlier agents. Use the Action button to execute actions.

Table 75-10 Legacy agent overview actions

Action	Description
Change Endpoint Server	Lets you change the Endpoint Server to which the agent connects.
	You can specify the primary Endpoint Server as well as secondary Endpoint Servers in case the primary server fails and the agent must switch connections.
Delete	Deletes the agent When you delete an agent, you remove that agent and all associated events from the Endpoint Server. It is no longer visible in the Enforce Server administration console. Deleting an agent from the Endpoint Server does not mean that it has been uninstalled from the endpoint.

Legacy agent overview actions (continued) Table 75-10

Action	Description
Disable	Disables the agent
	Disabling the agent does not delete the agent from the Endpoint Server. Disabling an agent disables all monitoring on that endpoint. The associated events are still visible on the Endpoint Server. Unlike deleted agents, disabled agents can be re-enabled.
Enable	Enables disabled agents
	Enabled agents automatically reconnect with the Endpoint Server and obtain the most current policies. Enabling an agent enables monitoring on that endpoint. Enabled agents can log events on the Endpoint Server.
	<b>Note:</b> Any updates to the associated policies are not sent to the agent until the agent is enabled and restarted.
Pull Logs	Lets you pull service logs and operational logs for the agent. You can pull either the service logs, or the operational logs, or both sets of logs.
	Pulling agent logs is a two-step process:
	<ul> <li>Pull the agent logs from the endpoint to the Endpoint Server</li> <li>Collect the agent logs from the Endpoint Server through the Enforce Server</li> </ul>
	When the logs are pulled from the endpoint, they are stored on the Endpoint Server in an unencrypted format. After you collect the logs from the Endpoint Server, the logs are deleted from the Endpoint Server and are stored only on the Enforce Server. You can only collect logs from one endpoint at a time.
	Access the logs from the Enforce Server Logs page. Go to: System > Servers > Logs > Collection.
	See "Collecting server logs and configuration files" on page 257.

Table 75-10	Legacy agent overview actions (continued)
Table / 2-10	Legacy agent overview actions (continued)

Action	Description
Remove Under Investigation	Removes the Under Investigation designation from the selected agents.
Reset Log Level	Resets the logging level for the specified agent to the default <b>INFO</b> level. Symantec Technical Support uses agent logs for troubleshooting purposes.  See "About Endpoint Agent logs" on page 1500.
Restart	Restarts the specified agent.
Set Log Level	Sets the logging level for the specified agent. Symantec Technical Support uses agent logs for troubleshooting purposes.
	Note: It is recommended to contact Symantec Technical Support before you change the log level for an agent.
	See "About Endpoint Agent logs" on page 1500.
Set Under Investigation	Sets an Under Investigation status on the selected agent.
	Specify agents as Under Investigation if you believe there is some sort of issue with the agent. You can set the Under Investigation status regardless of whether the agent is running, disabled, or shut down. An additional icon, a flag, appears next to the main status icon of the agent.
Shut Down	Shuts down the selected agent.

You can view the most current information regarding the agent actions in a knowledge base article. Log on to the DLP Knowledgebase at: https://kb-vontu.altiris.com and search for the article "About Symantec DLP Agent troubleshooting tasks." Or search for the article number: 54083.

# Agent task confirmation screen

Depending on the agent task you selected, you may see one of the following confirmation pages. Some of the confirmation pages request that you enter more information to complete the task. Other confirmation pages only require you to

confirm the task. The following table describes the different agent overview task confirmation pages:

Table 75-11 Agent task confirmation pages

Task	Page details
Delete	Confirm that you want to delete the Symantec DLP Agent.
	Click <b>OK</b> to confirm the deletion.
Change Endpoint Server	Enter the IP address or host name and port number to change the Endpoint Servers your DLP Agents report to.
	See "Changing the Endpoint Prevent Server" on page 1490.
Change Group	Select an agent group to where you want to move the selected agent.
	The agent is moved to the selected group after the agent connects to the Endpoint Server.
Restart	Click <b>OK</b> to confirm that you want to restart the Symantec DLP Agent.
Shut Down	Confirm that you want to shut down the selected agents. You must select one of the following options:
	<ul> <li>Shut down the DLP Agent and do not restart Agent if the endpoint computer restarts.</li> <li>The Symantec DLP Agent remains shut down if the endpoint computer restarts.</li> <li>Shut down the DLP Agent and restart Agent if the endpoint computer restarts. The Symantec DLP Agent is shut down but automatically restarts when the endpoint computer restarts.</li> </ul>
	After the agent shuts down, you cannot restart it from the Enforce Server administration console.
	Select the shutdown option and then click <b>OK</b> .

Agent task confirmation pages (continued) Table 75-11

Task	Page details
Pull Logs	Select the type of agent logs that you want, then click <b>OK</b> . You can select one of the following types of logs:
	<ul><li>Service Logs</li><li>Operational Logs</li></ul>
	You must select at least one type of log.
Disable	Confirm that you want to disable the Symantec DLP Agent. Disabling the agent does not delete it.
	Click <b>OK</b> to confirm.
	<b>Note:</b> After you disable an agent, configuration updates and Endpoint Discover requests from the Endpoint Server are not received.
Enable	Confirm that you want to enable the Symantec DLP Agent.
	Click <b>OK</b> to confirm.
	<b>Note:</b> After you enable the agent, restart it. Restarting the agent ensures that you have the latest policy, configuration updates, and Endpoint Discover requests.
Remove Under Investigation	No confirmation page for this task.
Reset Log Level	Reset the logging level for a Symantec Data Loss Prevention agent to the default <b>INFO</b> level. Symantec Technical Support uses agent logs for troubleshooting purposes.
Set Log Level	Set the logging level for a Symantec Data Loss Prevention agent. Symantec Technical Support uses agent logs for troubleshooting purposes.
	<b>Note:</b> It is recommended to contact Symantec Technical Support before you change the log level for an agent.
Set Under Investigation	No confirmation page for this task.

### **Changing the Endpoint Prevent Server**

The Change Endpoint Server task lets you change which Endpoint Prevent Servers your DLP Agents report to. While performing this task, you can also define alternate Endpoint Prevent Servers that the DLP Agents can connect to. The ability to define alternate Endpoint Prevent Servers enables:

- Redundancy in cases where the primary Endpoint Prevent Server goes offline.
- DLP Agents to connect to other Endpoint Prevent Servers when the endpoint is located in another geographic location or is moved to another policy group.
- DLP Agents to connect to alternate Endpoint Prevent Servers if the maximum number of DLP Agents are already connected to the primary Endpoint Prevent Server.

#### To change the Endpoint Prevent Servers that the DLP Agent reports to:

- Enter the IP address or host name for the primary Endpoint Prevent Server.
- 2 Enter the port number for the primary Endpoint Prevent Server.

Note: Port values must be between 1 and 65535.

- If you want to add an alternate Endpoint Prevent Server, click the plus sign (+) to add another entry.
- 4 Enter the IP address or the host name for the alternate Endpoint Prevent Server.
- 5 Enter the port number for the alternate Endpoint Prevent Server.

Note: Port values must be between 1 and 65535.

- 6 If you want to add an additional alternate Endpoint Prevent Server, repeat step
- If you have added too many Endpoint Prevent Server entries, you can delete 7 an entry by clicking the minus sign (-) next to the entry.
- If you are finished adding or changing the Endpoint Prevent Servers, click **OK** to submit your changes.

# Agent events

The Agent Events screen (Systems > Agents > Events) lists the events that have occurred on agents. These events can include changes in the database file,

connection, file-system driver, and service. You can filter and summarize the event list and click on individual event entries to see more details.

Event information is divided into several columns. Click any column header to sort entries alpha-numerically in that column. To sort in reverse order, click the column header a second time. By default, Symantec Data Loss Prevention lists events in order of the time they occurred.

Table 75-12 Agent Management Event screen

Entry	Description	
Туре	Displays the event type, which includes the following possible values:  Severe Agent Information OK	
Time	Displays the event date and time.	
Machine Name	Displays the endpoint IP address or host name.	
Category	Lists the event category, such as Agent Service Status, Connection Status, File-System Driver, or data store.	
Sub-Category	Displays the event sub-category, such as Connection Active or Connection Closed.	

You can click any event to display the agent event detail screen for that event.

See "Agent Event Detail screen" on page 1492.

You can filter the information that displays on the **Events** screen using a number of criteria, including date, computer name, and event type. Additionally, you can filter the agent events by specific sets of criteria relating to the Symantec DLP Agent. Summarizing and filtering the events lets you view the agent data in the order that you want. For example, you can summarize the agents by computer name and then filter by the most recently updated agents.

See "About filters and summary options for reports" on page 1046.

See "Troubleshooting agent alerts" on page 1493.

## Summarizing agent events

After you select and apply filtering and sorting criteria on the Events screen (System > Agents > Events), the Events screen displays a summary that matches your selections.

You can click each column to sort agents. Click a number to display agents that fit the criteria.

The far left column displays the sort option you selected in the **Summarize By** list.

Agent event summary Table 75-13

Column	Description	
Machine Name	Displays the computer names.	
Total	Lists the number of connected agents.	
Severe	Lists the number of agents with a warning status.	
Warning	Lists the number of agents with a warning status.	
Info	Lists the number of events associated with the agent. Click this number to display more information about the event or events.	

## **Agent Event Detail screen**

The Agent Event Detail screen displays all of the information available for the selected event. This screen is not editable.

Table 75-14 Agent Event Detail screen

	-	
Section	Title	Options
General	Туре	Indicates the general type of event that has occurred. The types possible events include:
		<ul> <li>Severe         Indicates an error that requires immediate attention.     </li> <li>Warning         Indicates a problem that is not severe enough to generate an error.     </li> <li>Info         Lists agent information.     </li> <li>Time         Provides the time the event occurred.     </li> <li>Machine Name         Provides the endpoint name.     </li> </ul>

Section	Title	Options
Message		<ul> <li>Provides details about the event.</li> <li>Summary         <ul> <li>A brief description of the event.</li> </ul> </li> <li>Detail             <ul></ul></li></ul>

Table 75-14 Agent Event Detail screen (continued)

See "Agent events" on page 1490.

## **Troubleshooting agent alerts**

The following section provides information on resolving agent alerts. You review agent alerts on the Agent Overview screen.

See "Agent Overview screen" on page 1457.

- Warning See Table 75-15 on page 1494.
- Critical See Table 75-16 on page 1496.

Table 75-15 lists agent alert details and provides information to troubleshoot and resolve agent issues that occur on Mac endpoints.

Table 75-15 Troubleshooting agents with Warning agent alert

Agent alert	Cause	Fix
DLP Outlook plug-in tampered with	The Outlook plug-in was modified, disabled, or deleted.	<ul> <li>To fix the issue:</li> <li>Restart Outlook.</li> <li>Verify that the Outlook plug-in Outlook2k3 Addin is enabled in Outlook.</li> <li>Run Outlook for at least 15 seconds, then restart Outlook.</li> <li>Confirm that the Outlook plug-in Outlook2k3 Addin is enabled.</li> </ul>
DLP Outlook plug-in installation failed	The Outlook plug-in installation failed.	Run the AgentInstaller.msi manually to repair the agent installation.
DLP Lotus Notes plug-in tampered with	The Lotus Notes plug-in was modified.	To fix the issue:  Restart Lotus Notes.  Uninstall the agent.  Restart the endpoint and install the agent.
DLP Lotus Notes plug-in installation failed	The Lotus Notes plug-in installation failed.	Run the AgentInstaller.msi manually to repair the agent installation.
DLP AIM plug-in tampered with	The AIM plug-in was modified or the plug-in installation failed.	To fix the issue:  Restart AIM.  Uninstall the agent.  Restart the endpoint and install the agent.
DLP AIM plug-in installation failed	The AIM plug-in installation failed.	Run the AgentInstaller.msi manually to repair the agent installation.
Active Directory user group resolution failed	Active Directory permissions conflict with Symantec Data Loss Prevention permissions. Also, Active Directory may be missing attributes.	Verify that the credentials that are passed to the agent have necessary permissions to extract logged-in user information from Active Directory.

Troubleshooting agents with Warning agent alert (continued) **Table 75-15** 

Agent alert	Cause	Fix
Agent is disabled by enforce user	The agent was disabled by the administrator who executed the <b>Disable</b> troubleshooting task on the <b>Agent List</b> screen.	Start the Windows agent using the <b>Agent List</b> screen. You can also start the agent by using the sc command.  See "Using the Agent List screen" on page 1460.  For Mac agents, you must use the agent_start tool to start the agent.  See "Starting DLP Agents that run on Mac endpoints" on page 1531.
Agent requires restart	The administrator can either disable or enable data loss monitoring on endpoints by executing the Disable or Enable troubleshooting task on the <b>Agent List</b> screen. Monitoring is enabled by default after the agent installation. However, when the administrator executes the Enable or Disable tasks and the agent is busy, the agent status may not update, so the agent remains in a Warning state.	Restart the agent on the <b>Agent List</b> screen.  See "Using the Agent List screen" on page 1460.
Agent crash dump available on endpoint for analysis	If the agent crashes, the Enforce Server displays the Warning agent alert type. In this scenario, a log file is created that Symantec Support can use to troubleshoot why the agent crashed.  Agent crashes can be caused by the following:  Temporary environment issues  Unknown agent issues  If the agent crashes often, contact Symantec support and provide the crash dump files available at the path  /AgentInstallDirectory/_MemDumpFiles/on the endpoint.	To fix the issue:  Shut down the agent on the Agent List screen. See "Using the Agent List screen" on page 1460.  Collect the crash dump files (*.dmp) from the path /AgentInstallDirectory/_MemDumpFiles/ on the respective endpoint.  Delete the crash dump files.  Restart the agent on the Agent List screen.

Troubleshooting agents with Warning agent alert (continued) **Table 75-15** 

Agent alert	Cause	Fix
Agent version is older than Enforce Server version	The agent is one version older than the Endpoint Server version to which it connects. For example, if the Endpoint Server is version 12.0 and the agent is 11.x, a <b>Warning</b> agent alert type displays. The features available in the Enforce and Endpoint Server are not available for these agents. Symantec Data Loss Prevention identifies these agents with a Warning alert because these agents do not provide current Symantec Data Loss Prevention features.	Upgrade the agent to the latest version.
Agent group attribute discovery failure	This alert occurs if the agent cannot collect required data from Active Directory, which prevents the Enforce Server from moving the agent into an agent group. The agent cannot collect data if there is an issue with Active Directory permissions or if required attributes are missing from Active Directory.	To fix the issue:  Verify Active Directory attribute query syntax.  Use AttributeQueryResolver.exe to test Active Directory queries that are defined in the Enforce Server.  See "About agent groups" on page 1443.
Agent group conflicts	The Endpoint Server automatically assigns the agent to an Agent Group depending on the endpoint attributes set during the Agent Group setup. If the endpoint meets multiple Agent Group conditions, the Warning alert is thrown.	To fix the issue:  Review Agent Group settings. See "About agent groups" on page 1443.  Re-create the agent group and use attributes that satisfy the conditions of the agent.

Troubleshooting agents with Critical agent alert **Table 75-16** 

Agent alert	Cause	Fix
Agent is not reporting	The agent has not reported to an Endpoint Server within the specified period of time. If the agent does not report after 18 hours, then Symantec Data Loss Prevention identifies the agent as not-reporting. Not-reporting agents do not receive the latest policies and configuration information, so they are marked with a Critical agent alert.	To fix the issue:  Verify that the endpoint where the agent is installed exists. If it does not exist, you can delete the agent from the Enforce Server.  See "Using the Agent List screen" on page 1460.  Verify that the agent is running on the endpoint.  Verify the network connection between the Endpoint Server and the endpoint.

Table 75-16 Troubleshooting agents with Critical agent alert (continued)

Agent alert	Cause	Fix
Agent version is not supported	The agent is two versions older than the Endpoint Server version to which it connects. For example, if the Endpoint Server is version 12.0 and the agent is 10.x, a <b>Critical</b> agent alert displays. The features available in Enforce and Endpoint Server are not available for these agents. Symantec Data Loss Prevention identifies these agents with a Critical alert because these agents do not provide current Symantec Data Loss Prevention features and may not operate as designed.	Upgrade the agent to the latest version.
File system driver is down	The agent service cannot communicate with the Symantec Data Loss Prevention driver installed on the endpoint.  Communication may not occur for the following reasons:  The file system drivers have been deleted.  Symantec Data Loss Prevention identifies the driver as invalid. This sometimes occurs when the driver has been modified.  Communication between Symantec Data Loss Prevention and the agent driver is broken due to attack.	To fix the issue:  Restart the endpoint. Reinstall the agent.

# About Symantec DLP Agent removal

You may need to uninstall the Symantec DLP Agent from your endpoints. You can uninstall Symantec DLP Agents in the following ways:

Table 75-17 Removing the Symantec DLP Agent

Removing a DLP Agent from a Windows endpoint

Removing DLP Agents from Windows endpoints using system management software

[Unresolved xref]

Removing a DLP Agent from a Mac endpoint

## Removing DLP Agents from Windows endpoints using system management software

Follow this procedure if you elected to hide the Symantec Data Loss Prevention service from the Add or Remove Programs list (ARP) during installation. Because the Symantec DLP Agent does not appear in the ARP, you cannot use the ARP list for the uninstallation process. You must use the MSI command to remove the Symantec DLP Agent. Only use the MSI command uninstallation if you have hidden the Symantec DLP Agent from the ARP during installation.

#### To remove the agent with the MSI command

- 1 Open the command prompt window.
- 2 Enter the string:

```
msiexec /x AgentInstall.msi
```

You can add several different options to this command prompt.

Click OK. 3

The Symantec DLP Agent uninstalls.

#### To remove the agent manually if the agent does not appear in the ARP

- Open the command prompt window. 1
- 2 Enter the following command where [quid] is the product code. You can locate the GUID from the Windows registry or in the uninstall agent.bat file.

You can add several other options to this command prompt:

```
msiexec /x {quid}
```

3 Enter any optional commands to the end of the command:

```
msiexec /x AgentInstall.msi
```

#### 4 Click OK.

You can add options to the uninstall command such as SilentMode or Logname. SilentMode allows the Symantec DLP Agent to uninstall without displaying a user interface on the desktop. The installation takes place in the background of the workstation and is not visible to the user. Logname Lets you set any log file you want. However, this option is only available if you have the original installer present. If you do not have the original installer, you must use the product code.

The code for a silent install is:

```
/ON:silentmode
```

The code for Logname is:

```
/L*V logname
```

msi.exe has several other options. For further options, see your MSI guide.

See "About Symantec DLP Agent removal" on page 1497.

#### Removing DLP Agents from a Windows 7 endpoint

If you uninstall the agents from an endpoint that runs Windows 7, you must run the command prompt in **Elevated Command Prompt** mode. This step is required because of the nature of the Windows operating system. You cannot install the agent using the install agent.bat script without first using the Elevated Command Prompt mode.

#### To initiate the Elevated Command Prompt mode on Windows 7

- 1 Click the Start menu.
- 2 In the Search programs and files field, type command prompt.
  - The **Command Prompt** program appears in the results list.
- Hold the Shift key and right-click the **Command Prompt** entry in the results list. Select either Run as Administrator or Run as different user.
- 4 If you selected Run as different user, enter the credentials for a user that has administrator privileges.
- The command prompt starts in Elevated Command Prompt mode. Install the 5 Symantec DLP Agents on the endpoint using this command prompt.

See "About Symantec DLP Agent removal" on page 1497.

## Removing a DLP Agent from a Windows endpoint

You can uninstall Symantec DLP Agents manually. Manual uninstallation is only possible if you configured the Symantec DLP Agent to appear in the endpoint Add or Remove Programs list during deployment.

Note: You uninstall Windows 7/8/8.1 agents in Elevated Command Prompt mode.

#### To uninstall the agent manually

- Go to Start > Control Panel and double-click Add or Remove Programs.
- 2 Select Agent Install.
- Click Remove.

See "About Symantec DLP Agent removal" on page 1497.

### Removing a DLP Agent from a Mac endpoint

You can uninstall the Mac DLP Agent by running the uninstaller tool from the default agent installation location: /Library/Manufacturer/Endpoint Agent.

#### To uninstall the DLP Agent from Mac endpoints

- 1 Open the Terminal app.
- 2 Run this command:

\$sudo ./uninstall agent

Note: You can review uninstall logs on the Terminal application by running this command: sudo ./uninstall agent -prompt=no -log=console. By default, logs are saved to the uninstall agent.log file

# About Endpoint Agent logs

Endpoint Agent logs contain service and operational data for every Endpoint Agent. Each Endpoint agent has multiple components that are logged. The amount of information that is logged can be configured by setting the log level for each Endpoint Agent component. After the log level for an Endpoint Agent component has been configured, the log can be collected and sent to Symantec Technical Support. Symantec Technical Support can use the log to troubleshoot a problem or to improve performance for a Symantec Data Loss Prevention Endpoint installation.

See "Setting the log levels for an Endpoint Agent" on page 1501.

See "Collecting server logs and configuration files" on page 257.

# Setting the log levels for an Endpoint Agent

You can configure the amount of data that is logged for an agent by specifying the log level for each agent component. Symantec Technical Support can use this data to troubleshoot or improve performance for a Symantec Data Loss Prevention Endpoint installation.

See "About Endpoint Agent logs" on page 1500.

Note: Symantec recommends that you contact Support before changing a log level for an agent.

#### To set the log levels for an agent

- From the Enforce Server administration console, navigate to **System > Agents** > Overview.
- 2 Click an agent status.
- 3 Select an agent.
- Select Troubleshoot > Set Log Level for current DLP Agents. Select Actions > Set Log Level for DLP Agents older than Symantec Data Loss Prevention version 12.5.
- 5 Select a log level from the **Log level** pull-down list.
- If you want to change the log level for all of the components for this agent, select All Agent Logger Components.
- If you change the log level for specific components of this agent, enter each component name into the provided field. When entering multiple component names, use a comma to separate each component name. Component names cannot exceed 255 characters.
- 8 Click **OK** to save your changes.

The **Agent List** screen displays an icon next to the agent to indicate the log level change. For DLP Agents older than Symantec Data Loss Prevention version 12.5, the Legacy Summary Reports screen displays an icon next to the agent to indicate the log level change.

It is recommended that you reset the agent log levels to the default settings after troubleshooting completes. Only general information about the agent is logged after the log levels are reset.

To reset the log levels for all the components of an Endpoint Agent to the default logging level

- 1 From the Enforce Server administration console, navigate to **System > Agents** > Overview.
- 2 Click an agent status.
- 3 Select an agent.
- 4 Select Troubleshoot > Reset Log Level for current DLP Agents or Actions > Reset Log Level for DLP Agents older than Symantec Data Loss Prevention version 12.5.

The Agents Overview screen displays an icon next to the agent to indicate the updated the log level.

# Using application monitoring

This chapter includes the following topics:

- About monitoring applications
- About adding applications
- Adding an application
- About Application File Access monitoring
- Implementing Application File Access monitoring

# About monitoring applications

Symantec Data Loss Prevention enables you to monitor applications for CD/DVD burning, IM, email, or HTTP/S clients. By default, Symantec Data Loss Prevention monitors applications such as Apple iTunes, Microsoft Outlook, or Mozilla Firefox. You use the Application Monitoring screen (**System > Agents > Application Monitoring**) to review and change application monitoring settings.

You can use monitor settings to control how and if the DLP Agent monitors the following activities:

- Data moving across the network
- Data being printed or faxed
- Data moving to and from an endpoint Clipboard
- Data moving to applications
- Data being written to a CD or DVD

Data moving between USB, network share, and local disks and an application

You can add applications your company uses that are not listed on the Application Monitoring page. For example, if your company uses Skype, you can add the application to the Application Monitoring page. After you add Skype, Symantec Data Loss Prevention monitors the files sent by the client over the network.

Note: You can remove any application that you add, but you cannot remove a system-provided application.

See "Adding an application" on page 1506.

See "Implementing Application File Access monitoring" on page 1510.

# Changing application monitoring settings

You can configure global changes to the applications that display by default on the Application Monitoring screen. You can associate blacklist or whitelist metadata to network monitoring, CD/DVD applications, and the applications that use print/fax or Clipboard functions. You can also specify if you do not want Symantec Data Loss Prevention to monitor applications for network, print/fax, Clipboard, or file system activities. For example, you may want to exclude Clipboard activities on Microsoft Outlook. You would edit the settings for Microsoft Outlook to exclude Clipboard activity on the **Application Information** screen.

#### To change application monitoring settings:

- Locate and click the application for which you want to change settings. 1
- 2 On the **Application Information** screen, make changes to the following items:

**Network Access** Monitors data moved over the network. The network includes

HTTP and FTP.

Print/Fax Monitors data that is printed or faxed.

Send to Clipboard Monitors data that resides on the endpoint Clipboard.

Filesystem Activity Monitors data moving between USB, network share, and local

disks and an application.

3 If you selected Filesystem Activity, you can select one of the following options:

Monitor Application Select Application File Access to monitor the files that the File Access application opens or reads. See "About Application File Access monitoring" on page 1509. Select CD/DVD to monitor the files that the application writes to Monitor writing to

Select an item to define how Symantec Data Loss Prevention monitors files 4 that are moved using applications.

a CD/DVD drive.

Select the File Read option. File Read is the recommended selection File Read because it provides better performance.

> When this option is selected, the file contents are monitored when the application reads the file.

File Open Select the **File Open** option only if the application hangs or crashes.

> When this option is selected, the application does not open a file if it contains sensitive information. However, Symantec Data Loss Prevention scans the file regardless of whether the application reads the content, which decreases performance.

Save your changes.

CD/DVD

See "About monitoring applications" on page 1503.

# About adding applications

You can use the **Application Information** screen to add applications to monitoring policies. By default, DLP Agents monitor Clipboard, print, network (HTTP and FTP), and file system (removable disc, local drive, and network share) activity on all applications. You add applications when you want DLP Agents to monitor files that applications open or read. You can also add applications when you want to prevent Symantec Data Loss Prevention from monitoring the application.

The following table lists the types of applications you can add:

Table 76-1 Application types you can add

Application type	Example
CD/DVD	Roxio

**Table 76-1** Application types you can add (continued)

Application type	Example
Internet browsers	Google Chrome
IM	Skype
SMTP	Mozilla Thunderbird

See "Adding an application" on page 1506.

See "Using the GetAppInfo tool" on page 1508.

# Adding an application

You can add applications to be monitored that are not already listed on the Application Monitoring screen.

See "About adding applications" on page 1505.

Adding an application

- Go to System > Agents > Application Monitoring.
- 2 Click **Add Application** to display the Application Information page.

#### 3 Enter information.

In addition to the **Name** field, you must enter information in at least one of either the Binary Name, Internal Name, or Original Filename fields.

See "Using the GetAppInfo tool" on page 1508.

Name Enter the application name. You must enter information in this field.

Binary Name

Enter the binary file name. Include an escape character (\) between the application name and the file extension. For example, if you want to add

Firefox, you enter firefox\.exe.

Internal Name

Enter the application name.

Original Filename Enter the application file name. Include an escape character (\) between the application name and the file extension. For example, if you plan to

add Firefox, you enter firefox\.exe.

**Publisher** Name

Enter a publisher name. This field is optional.

If you enter the Publisher Name, you can choose to select the **Verify** publisher name option. This option ensures that the publisher name of the application is correct. Using the **Verify publisher name** option may affect performance as it increases system resources.

Additionally, you can add details about the publisher name for the application. The publisher name details the maker of the software. Adding the publisher name lets Symantec Data Loss Prevention verify the application even if the binary name has been changed. Primarily, the publisher name is used for identifying Symantec processes. However, you can add the publisher name for any of your applications. Adding the publisher name is optional.

4 Under the Application Monitoring Configuration section, select one or more of the following monitoring options:

Network Monitors the data moved over the network. The network includes HTTP

Access and FTP

Print/Fax Monitors data that is printed or faxed.

Send to Monitors data that resides on the endpoint Clipboard. Clipboard

Filesystem Monitors data moving between USB, network share, and local disks Activity and an application.

5 If you selected **Filesystem Activity**, you can select one of the following options:

Monitor Application Select Application File Access to monitor the files that the File Access application opens or reads.

See "About Application File Access monitoring" on page 1509.

Select CD/DVD to monitor the files that the application writes to Monitor writing to CD/DVD or reads from a CD/DVD drive.

Select an item to define how Symantec Data Loss Prevention monitors files 6 that are moved using applications.

File Read Select the File Read option. File Read is the recommended selection because it provides better performance.

> When this option is selected, the file contents are monitored when the application reads the file.

File Open Select the File Open option only if the application hangs or crashes.

When this option is selected, the application does not open a file if it contains sensitive information. However, Symantec Data Loss Prevention scans the file regardless of whether the application reads the content, which decreases performance.

7 Save your changes.

See "About monitoring applications" on page 1503.

# Using the GetAppInfo tool

You can use the GetAppInfo.exe tool to generate application information. You use this tool when you add applications and use the Application Monitoring feature. The Application Monitoring feature monitors data that users move to applications.

Locate this application in the SymantecDLPWinAgentTools 12.5.zip in the DLP\Symantec DLP 12 Win\12.5 Win\Endpoint\x86 **or** \x64 **directory**.

#### To use the GetAppInfo tool:

- 1 Launch GetAppInfo.exe.
- 2 Enter the path to the application or click **Browse** and navigate to it.
- 3 Click Get Info.

The tool displays the following application information:

Comments

- InternalName
- CompanyName
- LegalCopyright
- **ProductVersion**
- FileDescription
- LegalTrademarks
- PrivateBuild
- **FileVersion**
- OriginalFilename
- SpecialBuild
- PublisherName
- Retain the application information the tool displays. You use the application information when you add an application on the Application Monitoring screen.

See "Adding an application" on page 1506.

See "About Application File Access monitoring" on page 1509.

# About Application File Access monitoring

When you enable the Application File Access feature, the DLP Agent monitors data leaving applications on endpoints. You enable this feature by adding the protocol that is labeled Protocol or Endpoint Monitoring protocol and setting response rules in a policy. You then enable the Application File Access feature in the agent configuration.

Note: You cannot use the Application File Access feature to monitor inline data transfers using browsers (HTTPS) or instant messenger.

You can enable default applications on the **Application Monitoring** screen. You can also set Symantec Data Loss Prevention to monitor the applications not found on the **Application Monitoring** screen by adding them.

If a user transfers a file containing sensitive information, a notification displays on the endpoint. Depending on your policies and Endpoint Prevent response, access to the file will be denied. You can review Application File Access incidents on the Incidents > Endpoint screen.

See "Implementing Application File Access monitoring" on page 1510.

See "Adding agent configurations" on page 1406.

See "Adding an application" on page 1506.

# Implementing Application File Access monitoring

You complete a number of steps to implement the Application File Access feature. Refer to See Table 76-2 on page 1510. for steps to complete the process.

Enabling the feature potentially affects application performance on endpoints. You can use environment variables in path filters to specify file locations to monitor, which helps application performance.

See "Using environment variables in Endpoint Discover scans" on page 1395.

Table 76-2 Implementing Application File Access

Step	Action	Description
1	Create a new policy or update an existing policy.	You enable the Protocol or Endpoint Monitoring protocol, then select options to configure Application File Access.
		See "Configuring policy rules" on page 330.
2	Set response rules for the policy.	See "Manage response rules" on page 889.
3	Add the policy to an Endpoint Discover target or confirm that an existing policy is added to a target.	See "Network Discover scan target configuration options" on page 1191.
4	Enable the Application File Access feature in the endpoint configuration.	Use environment, file, and folder filters to optimize file monitoring performance. The Application File Access feature monitors every file that an application opens or reads, which can reduce application performance and create false positives. You can use environment variables to specify locations where sensitive data is potentially located.
		See "Adding agent configurations" on page 1406.
		See "Configuring file filters" on page 1412.

Implementing Application File Access (continued) **Table 76-2** 

Step	Action	Description
5	Add an application to the Application Monitoring screen.	Many applications are listed in the Application Monitoring screen. If you add an application, you must enable the Monitor Application File Access feature and select an activity to monitor, either Read or Open.  See "Adding an application" on page 1506.

# Working with Endpoint FlexResponse

This chapter includes the following topics:

- About Endpoint FlexResponse
- Deploying Endpoint FlexResponse
- About deploying Endpoint FlexResponse plug-ins on endpoints
- Deploying Endpoint FlexResponse plug-ins using a silent installation process
- About the Endpoint FlexResponse utility
- Deploying an Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility
- Enabling Endpoint FlexResponse on the Enforce Server
- Uninstalling an Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility
- Retrieving an Endpoint FlexResponse plug-in from a specific endpoint
- Retrieving a list of Endpoint FlexResponse plug-ins from an endpoint

# About Endpoint FlexResponse

Symantec Data Loss Prevention provides a set of response rule actions that you can specify to remediate an incident. These provided actions include logging, sending an email, blocking an end-user action, notifying a user, and other responses.

You can also use Endpoint FlexResponse plug-ins to provide additional response actions. These plug-ins contain custom instructions for remediation actions that are

executed on endpoints. Endpoint FlexResponse rules are only applicable to Automated Response rules. You cannot create Endpoint FlexResponse rule actions for Smart Response rules.

Symantec Data Loss Prevention customers can contact Symantec or Symantec partners to obtain Endpoint FlexResponse plug-ins. In addition, developers with a knowledge of the Python programming language can create custom Endpoint FlexResponse plug-in scripts using a Symantec-provided API. These custom remediation actions can include encryption, applying Digital Rights Management (DRM), or redacting confidential information.

You use the Endpoint FlexResponse utility to deploy Endpoint FlexResponse plug-ins on endpoints in your Symantec Data Loss Prevention deployment where you require Endpoint FlexResponse actions. You can deploy the plug-ins manually using the Endpoint FlexResponse utility, or you can use system management software (SMS) to distribute the utility and deploy the plug-ins. After you deploy an Endpoint FlexResponse plug-in on an endpoint, you use the Enforce Server administration console to add an Endpoint: FlexResponse action to a response rule, and then you add the response rule to an active policy.

Figure 77-1 shows the sequence of activities that result in an Endpoint FlexResponse action.

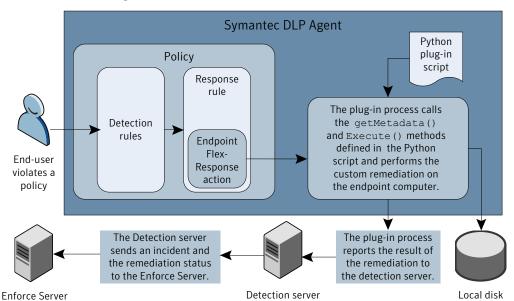


Figure 77-1 Endpoint FlexResponse plug-in process

You can use Endpoint FlexResponse rules on the following types of endpoint destinations and protocols:

Endpoint Discover

Note: Endpoint FlexResponse is currently unavailable for Endpoint Discover scans that run on Mac agents.

- Local drive monitoring
- Removable storage devices
- SMTP
- HTTP(S)

# **Deploying Endpoint FlexResponse**

Follow the steps provided here to deploy Endpoint FlexResponse plug-ins.

**Table 77-1** Deploying Endpoint FlexResponse

Step	Action	Description
Step 1	Obtain (or create) an Endpoint FlexResponse plug-in zip file.	Contact a Symantec partner or Symantec sales representative.
		Endpoint FlexResponse plug-ins are not available with the default Symantec Data Loss Prevention installation.
Step 2	Configure any Endpoint credentials on the Enforce Server.	See "Configuring endpoint credentials" on page 132.
		This step is optional.
Step 3	Deploy the plug-in to your endpoints using the Endpoint FlexResponse utility and third-party systems management software (SMS).	See "About deploying Endpoint FlexResponse plug-ins on endpoints" on page 1515.
Step 4	Enable Endpoint FlexResponse actions on your Enforce Server.	See "Enabling Endpoint FlexResponse on the Enforce Server" on page 1519.
Step 5	Add Endpoint FlexResponse actions to your response rules.	See "Adding a new response rule" on page 890.

# About deploying Endpoint FlexResponse plug-ins on endpoints

You must install Symantec DLP Agents on the endpoints before deploying Endpoint FlexResponse plug-ins. The Agents must be connected to an active Endpoint Server.

See the Symantec Data Loss Prevention Installation Guide for information on how to install the agents.

You must deploy Endpoint FlexResponse plug-ins on each endpoint where you require Endpoint FlexResponse actions. You can use a manual installation or a silent installation method to deploy the plug-in. Silent installation methods involve using systems management software (SMS), to distribute and install software on all of your endpoints. You may need to create SMS scripts to access the installation folder.

This section assumes that you have created or otherwise obtained an Endpoint FlexResponse plug-in that is packaged as a ZIP file.

Deploying an Endpoint FlexResponse plug-in on endpoints requires the following steps:

Step 1	Copy the Endpoint FlexResponse utility to your endpoints.
	See "About the Endpoint FlexResponse utility" on page 1516.
Step 2	Copy any third-party Python modules that your plug-in requires to your endpoints.
Step 3	Enable Endpoint FlexResponse on the Enforce Server. See "Enabling Endpoint FlexResponse on the Enforce Server" on page 1519.
Step 4	Deploy the Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility. $(flrinst.exe)$ . Use one of the following options:

- Deploy your plug-in manually on a single endpoint. This option is most useful when you are developing or testing an Endpoint FlexResponse plug-in.
  - See "Deploying an Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility" on page 1518.
- Deploy your plug-in using a silent installation process and SMS software. This option is most useful when you are deploying a production-ready Endpoint FlexResponse plug-in. See "Deploying Endpoint FlexResponse plug-ins using a silent

installation process " on page 1516.

Step 5

Create response rules that use **Endpoint: FlexResponse** actions that reference the plug-in, and add these rules to an active policy.

See "Implementing policy detection" in the Symantec Data Loss Prevention System Administration Guide.

# Deploying Endpoint FlexResponse plug-ins using a silent installation process

You can use system management software (SMS) to deploy Endpoint FlexResponse plug-ins on multiple endpoints. Although the details of creating installation scripts for SMS software are beyond the scope of this document, note the following requirements:

- You must install Symantec DLP Agents on the endpoints before deploying Endpoint FlexResponse plug-ins. The Agents must be connected to an active Endpoint Server.
- You must install the Endpoint FlexResponse utility (flrinst.exe) on each endpoint where you will deploy Endpoint FlexResponse plug-ins.
- You must make the Endpoint FlexResponse package (a .zip file) available to each endpoint. You can copy the package to each endpoint, or you can make the package available on a network drive that is accessible by all endpoints.
- To deploy your plug-in, use the command-line options of the Endpoint FlexResponse utility when creating your installation scripts. See Table 77-3 on page 1517.
- Remove the Endpoint FlexResponse utility after deploying your plug-in. If you leave the utility installed on the endpoints, a malicious user could use the utility to uninstall or alter your Endpoint FlexResponse plug-in.

See "About the Endpoint FlexResponse utility" on page 1516.

See your individual SMS application documentation for more information on how to deploy using SMS.

The Endpoint FlexResponse utility is only available through Symantec and Symantec partners. It is not included with the Symantec Data Loss Prevention distribution.

# About the Endpoint FlexResponse utility

You use the Endpoint FlexResponse utility to manage Endpoint FlexResponse plug-ins. The Endpoint FlexResponse utility is not part of the default Symantec Data Loss Prevention download and is only available through Symantec or Symantec partners.

Before you run the utility, package your Python scripts into a single ZIP file.

Endpoint FlexResponse utility actions Table 77-2

Action	Description
Deploy (Install) plug-ins	Use the install option to deploy plug-ins on an endpoint.
Uninstall plug-ins	Use the uninstall option to uninstall plug-ins from an endpoint.
Retrieve deployed plug-ins	Use the retrieve option to retrieve a specific plug-in that has already been deployed on an endpoint.
See a list of deployed plug-ins	Use the list option to retrieve a list of all plug-ins that are deployed on a specific endpoint. The list contains the names of the deployed plug-ins.

The Endpoint FlexResponse utility must be run from the folder where the Symantec DLP Agent is deployed. The location of this folder is configurable. By default, the directory is located at:

c:\Program Files\Manufacturer\Endpoint Agent\

The name of the utility is flrinst.exe. The utility uses the following syntax:

flrinst.exe -op=install|uninstall|retrieve|list -package=<package name> -p=<Tools password>

Table 77-3 Endpoint FlexResponse Utility options

Option	Description
-op=install uninstall retrieve list	Use one of the following arguments:
	<ul> <li>install—deploys a plug-in</li> <li>uninstall—removes a plug-in</li> <li>list—displays a list of deployed plug-ins</li> <li>retrieve—retrieves a plug-in and saves it as an editable text file. The text file is contained in a ZIP file that is saved in the directory where the utility was run.</li> </ul>

Option	Description
-package= <package_name></package_name>	When you specify the <code>-op=install</code> option, specifies the path to the package (a ZIP file) that contains the Endpoint FlexResponse plug-in. The package name is case sensitive.
	When you specify either the -op=retrieve or -op=uninstall option, specifies the name of the package.
-p= <tools_password></tools_password>	Specify the Tools password that has been configured for your Symantec Data Loss Prevention deployment.
	If a Tools password has not been configured, use the default password, "VontuStop".
	<b>Note:</b> As of Symantec Data Loss Prevention version 11.1.1, the password is no longer optional.

Table 77-3 Endpoint FlexResponse Utility options (continued)

If you have created a Tools password for your Symantec Data Loss Prevention deployment, pass this password to the Endpoint FlexResponse utility with the -p option. This password is required to install and uninstall a plug-in. You configure a Tools password during Symantec Data Loss Prevention installation. For more information, see the Symantec Data Loss Prevention Administration Guide.

If you have not configured a Tools password, an end user can retrieve and modify previously-installed plug-ins using the default password, Vontustop. Symantec recommends that you configure a Tools password to prevent such tampering. Alternately, you can set your SMS application to remove the Endpoint FlexResponse Utility after you have used it. Removing the utility prevents any unauthorized modification or uninstallation of your plug-ins.

# Deploying an Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility

You use the Endpoint FlexResponse utility to deploy Endpoint FlexResponse plug-ins. The plug-ins must be in a .zip package format.

#### To deploy an Endpoint FlexResponse plug-in

On an endpoint, open a command window and navigate to the Symantec DLP Agent installation tools directory. The default location of this directory is

```
c:\Program Files\Manufacturer\Endpoint Agent\
```

2 Enter the following command:

```
flrinst.exe -op=install
             -package=<path to plug-in>
             -p=<myToolsPassword>
```

#### Where:

- <myToolsPassword> is the Tools password for your Symantec Data Loss Prevention deployment. If you have not specified a Tools password, use the default password: VontuStop.
- path to plug-in name> is the full path to the plug-in .zip file.

#### For example:

```
flrinst -op=install -package=c:\installs\myFlexResponse plugin.zip
-p=myToolsPassword
```

See "Deploying Endpoint FlexResponse" on page 1514.

See "About the Endpoint FlexResponse utility" on page 1516.

# **Enabling Endpoint FlexResponse on the Enforce** Server

Before you can use Endpoint FlexResponse plug-ins in your response rules, you must enable Endpoint FlexResponse functionality through the Enforce Server. By default, Endpoint FlexResponse functionality is not enabled. You enable Endpoint FlexResponse functionality through the Advanced Agent Settings.

#### To enable Endpoint FlexResponse functionality

- Open the Enforce Server administration console and navigate to: **System >** Agents > Agent Configuration and open the Agent configuration that is currently applied to the Endpoint Server that is connected to the Agents where you are deploying the Endpoint FlexResponse plug-in.
- 2 Click the Advanced Agents Settings tab.
- 3 Find the PostProcessor.ENABLE FLEXRESPONSE.int setting.

- Change the setting to 1.
- Click Save and Apply.

See "Adding a new response rule" on page 890.

See "Deploying Endpoint FlexResponse" on page 1514.

See "About deploying Endpoint FlexResponse plug-ins on endpoints" on page 1515.

# Uninstalling an Endpoint FlexResponse plug-in using the Endpoint FlexResponse utility

To uninstall an Endpoint FlexResponse plug-in from an endpoint

- On an endpoint, open a command window and navigate to the Symantec DLP Agent installation directory. The default location of this directory is: c:\Program Files\Manufacturer\Endpoint Agent.
- 2 Enter the following command:

```
flrinst.exe -op=uninstall
           -package=<Plug-in name>
            -p=<mvToolsPassword>
```

#### Where:

- <Plug-in name> is the name of the plug-in package .zip file.
- <myToolsPassword> is the Tools password for your Symantec Data Loss Prevention deployment. If you have not specified a Tools password, use the default password: VontuStop.

#### For example:

```
flrinst -op=uninstall -package=myFlexResponse plugin.zip
  -p=myToolsPassword
```

# Retrieving an Endpoint FlexResponse plug-in from a specific endpoint

Use the following procedure to retrieve a specific plug-in from an endpoint. You can only use the retrieve function on a single endpoint at a time. The plug-in appears in the Symantec DLP Agent installation directory as a .zip file. The plug-in script is a plain-text file that has a .py extension and is located inside a .zip file.

You can edit the plug-in by editing the .py file. If you make edits, you must re-package the ZIP file and re-deploy the plug-in to the endpoint before the edits take effect. Modified plug-ins only affect the individual endpoints where they were modified.

#### To retrieve an Endpoint FlexResponse plug-in from a specific endpoint

On the endpoint, open a command prompt window and navigate to the Symantec DLP Agent installation directory:

```
The default location of this directory is c:\Program
Files\Manufacturer\Endpoint Agent\
```

Enter the following command:

```
flrinst -op=retrieve -package=<Plug-in name> -p=<myToolsPassword>
```

#### Where:

- <myToolsPassword> is the tools password for your Symantec Data Loss Prevention deployment. If you have not specified a Tools password, use the default password: VontuStop.
- <plug-in name> is the name of the plug-in .zip file.

#### For example:

```
flrinst -op=retrieve -package=myFlexResponse plugin.zip
-p=myToolsPassword
```

# Retrieving a list of Endpoint FlexResponse plug-ins from an endpoint

Use the following procedure to retrieve a list of plug-ins that have been deployed on a specific endpoint. You can only use the list function on individual endpoints. You cannot use the list function on a set of endpoints.

The list of plug-ins contains only the name of the plug-in package. The list does not contain any type of description about the plug-ins. Symantec recommends that you use descriptive names for your plug-ins so that you can recognize them within the list.

#### To retrieve the list of Endpoint FlexResponse plug-ins from an endpoint

- 1 On an endpoint, open a command window and navigate to the Symantec DLP Agent installation tools directory. The default location of this directory is c:\Program Files\Manufacturer\Endpoint Agent\.
- 2 Enter the following command:

```
flrinst.exe -op=list -p=<myToolsPassword>
```

Where: <myToolsPassword> is the Tools password for your Symantec Data Loss Prevention deployment. If you have not specified a Tools password, use the default password: VontuStop.

For example:

```
flrinst -op=list -p=myToolsPassword
```

The list of deployed Endpoint FlexResponse plug-ins displays in the command window.

# Using Endpoint tools

This chapter includes the following topics:

About Endpoint tools

# **About Endpoint tools**

Symantec Data Loss Prevention provides a number of tools to help you work with Symantec DLP Agents. See the *Acquiring Symantec Data Loss Prevention Software* document for information on obtaining the files that contain these tools.

Move these tools to a secure directory. These Endpoint tools work with the keystore file that is found in the Agent Install directory. The tools and the keystore file must be in the same folder to function properly. Each tool requires a password to operate. A universal tools password is generated during your installation.

The following list contains some of the tasks that you can complete using endpoint tools:

**Table 78-1** Endpoint tools task list

Task	Tool name and location	Additional information
Shut down the agent and the watchdog services	service_shutdown  Available for Windows agents in the  Symantec_DLP_12.5_Agent_Win-IN.zip file.	Shutting down the agent and the watchdog services

Endpoint tools task list (continued) Table 78-1

Task	Tool name and location	Additional information
Inspect database files that are accessed by the agent	vontu_sqlite3  Available for Windows agents in the Symantec_DLP_12.5_Agent_Win-IN.zip file.  Available for Mac agents in Symantec_DLP_12.5_Agent_Mac-IN.zip file.	
View extended log files	logdump  Available for Windows agents in the  Symantec_DLP_12.5_Agent_Win-IN.zip file.  Available for Mac agents in the  Symantec_DLP_12.5_Agent_Mac-IN.zip file.	Viewing extended log files
Generate uninstallation passwords for your agents	UninstallPwdKeyGenerator  Available for Windows agents in the  Symantec_DLP_12.5_Agent_Win-IN.zip file.	Creating passwords with the password generation tool
Generate third-party application information	GetAppInfo Available for Windows agents in the Symantec DLP_12.5 Agent_Win-IN.zip file.	Using the GetAppInfo tool
Start DLP Agents that are installed on Mac endpoints	Available for Mac agents in the AgentInstaller_Mac64.zip file. This file is created after you complete the agent installation package process. See "Generating agent installation packages" in the Symantec Data Loss Prevention Installation guide for more information.  Note: You must unzip this file to a Mac endpoint. You cannot use the tool if it is unzipped to a Windows endpoint.	Starting DLP Agents that run on Mac endpoints

### Using Endpoint tools with Windows 7/8/8.1

If you use Endpoint tools on a computer that runs Windows 7/8/8.1, run the command prompt in the Elevated Command Prompt mode. This procedure is required because of the nature of the Windows operating system. You cannot run the Endpoint tools without using the Elevated Command Prompt mode.

#### To initiate the Elevated Command Prompt mode on Windows 7

- 1 Click the Start menu.
- 2 In the Search programs and files field, enter command prompt.
  - The Command Prompt program appears in the results list.
- Hold the Shift key and right-click the **Command Prompt** entry in the results list. Select either Run as Administrator or Run as different user.
- If you selected Run as different user, enter the credentials for a user that has administrator privileges.

#### To initiate the Elevated Command Prompt mode on Windows 8/8.1

- Display the Command Prompt.
  - In Desktop mode, right-click on the Windows icon and select Command Prompt (Admin), then click the Start menu.
  - In Metro mode, enter cmd in the Search programs and files field.
- 2 Hold the Shift key and right-click **Command Prompt** in the results list.
- 3 Select Run as Administrator.

### Shutting down the agent and the watchdog services

The Service Shutdown.exe tool shuts down the Symantec DLP Agent and watchdog services. As a tamper-proofing measure, it is not possible for a user to individually stop either the Symantec DLP Agent or watchdog service. This tool enables an administrator to stop both Symantec Data Loss Prevention services at the same time.

#### To run the Service\_Shutdown.exe tool

From the installation directory, run the following command:

```
service shutdown [-p=password]
```

where the installation directory is the directory where you installed Symantec Data Loss Prevention and [-p=password] is the password you previously specified. If you do not enter a password, you are prompted to input a password. The default password is VontuStop.

You must run the Service Shutdown.exe tool from the same directory as the Symantec DLP Agent keystore file.

See "About Endpoint tools" on page 1523.

# Inspecting the database files accessed by the agent

The vontu sqlite3 tool enables you to inspect the database files that the Symantec DLP Agent uses. It provides an SQL interface to query database files and update database files. Without this tool, you cannot view the contents of a database file because it is encrypted. Use this tool when you want to investigate or make changes to the Symantec Data Loss Prevention files.

Note: You can use this tool to view DLP Agent log files on Mac endpoints. You must have root or sudo access to make changes to the agent database.

#### To run the vontu\_sqlite3.exe tool

- Run one of the following scripts from the Symantec Data Loss Prevention Agent installation directory:
  - For Windows agents run the following command:

```
vontu sqlite3 -db=database file [-p=password]
```

where database file is your database file and password is your specified tools password.

The Symantec Data Loss Prevention database files for Windows agents are located in the Symantec DLP Agent installation directory and end in the \*.ead extension. After you run the command, you are prompted for your password.

For Mac agents run the following command:

```
sudo ./vontu sqlite3 -db=database file [-p=password]
```

where database\_file is your database file and password is your specified tools password.

You run this command using the Terminal application. The vontu sqlite3 tool is located at /Library/Manufacturer/Endpoint Agent/.

2 Enter the default password Vontustop unless you have already created a unique password.

You are provided with a shell to enter SQL statements to view or update the database.

Refer to http://www.sqlite.org/sqlite.html for complete documentation about what commands are available in this shell.

See "About Endpoint tools" on page 1523.

# Viewing extended log files

The logdump.exe tool lets you view the extended log files for Symantec Data Loss Prevention Agents. Extended log files are hidden for security reasons. Generally, you only need to view log files with Symantec Data Loss Prevention support personnel. Without this tool, you cannot view any Symantec Data Loss Prevention Agent log files.

Note: You can use this tool to view DLP Agent log files on Mac endpoints. You must have root or sudo access to make changes to the agent database.

#### To run the log dump tool

- Run one of the following scripts from the Symantec Data Loss Prevention Agent installation directory:
  - On Windows agents:

```
logdump -log=log file [-p=password]
```

where log\_file is the log file you want to view and password is the specified tools password. All Symantec Data Loss Prevention extended log files are present in the Symantec Data Loss Prevention Agent installation directory. The files have names of the form edpa extfile\_number.log. After you run this command, you can see the de-obfuscated log.

Note: When using Windows PowerShell to run logdump.exe, quotes are required around the log file. For example, run:

```
logdump "-log=log file" [-p=password]
```

On Mac agents:

```
sudo ./logdump -log=log file [-p=password]
```

where log\_file is the log file you want to view and password is the specified tools password.

All Symantec Data Loss Prevention extended log files are present in the Symantec Data Loss Prevention Agent installation directory. The files have names of the form edpa extfile number.log. After you run this command, you can see the de-obfuscated log.

2 (Optional) Print the contents of another log from this view.

#### To print the contents of another log

From the command window, run:

```
logdump -log=log file -p=password > deobfuscated log file name
```

Enter the password again to print the log.

See "About Endpoint tools" on page 1523.

## About the Device ID utility

Symantec Data Loss Prevention provides the DeviceID.exe utility to assist you with configuring endpoint devices for detection.

See "About endpoint device detection" on page 634.

The DeviceID utility scans the computer for all connected devices and reports the Device Instance ID string for each device that is detectable.

See "Using the Device ID utility" on page 1529.

Device ID utility example output Table 78-2

Result	Description	
Volume	The volume or mount point that the DeviceID.exe tool found.	
	For example:	
	Volume: E:\	
Dev ID	The Device Instance ID for each device.	
	For example:	
	USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\5F73HF00Y9DBOG0DXJ	

Table 78-2 Device ID utility example output (continued)

Result	Description	
Regex	The regular expression to detect that device instance.	
	For example:	
	USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\5F73HF00Y9DBOG0DXJ	

#### Using the Device ID utility

Use the Device ID utility to extract Device Instance ID strings and to determine what devices the system can recognize for detection.

See "About the Device ID utility" on page 1528.

See "About endpoint device detection" on page 634.

#### To use the Device ID utility

Obtain the DeviceID.exe utility.

This utility is available with the Endpoint Sever utilities package.

See "About Endpoint tools" on page 1523.

- 2 Copy the DeviceID.exe utility to a computer where you want to determine Device IDs.
- 3 Install the devices you want to examine onto the computer where you copied the DeviceID.exe utility.

For example, plug in one or more USB devices, connect a hard drive, etc.

Run the DeviceID.exe utility from the command line.

For example, if you copied the DeviceID.exe utility to the C:\temp directory, issue the follow command:

C:\temp>DeviceID

To output the results to a file, issue the following command:

C:\TEMP>DeviceID > deviceids.txt

The file appears in the C:\temp directory and contains the output from the DeviceID process.

5 View the results of the DeviceID process.

The command prompt displays the results for each volume or mount point.

See Table 78-2 on page 1528.

Use the DeviceID utility to evaluate the proposed regex string against a device that's currently connected.

See Table 78-3 on page 1530.

Use the regular expression patterns to configure endpoint devices for detection. See "Creating and modifying endpoint device configurations" on page 641.

**Table 78-3** Device ID regex evaluation

Command parameters	Example
DeviceID.exe [-m] [Volume] [Regex]	DeviceID.exe -m E:\ "USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\.*"  Note: The regex string needs to be inside quotation marks.
Returns	Match! or Not match!

# Creating passwords with the password generation tool

Use the uninstallation password generator tool to create a unique password key.

The name of the uninstallation password generator tool is UninstallPwdKeyGenerator.

The uninstallation password prevents unauthorized users from removing the Symantec DLP Agent. The UninstallPwdKeyGenerator tool works with the PGPSdk.dll file to create unique passwords. The tool and the file must be located in the same tools directory to function. The Uninstall PwdKeyGenerator tool and the PGPSdk.dll file are located in the Administrator tool directory by default.

Note: The UninstallPwdKeyGenerator tool only works in Microsoft Windows environments. You cannot use this tool with any other operating system.

#### To create an uninstallation password

- From a command window, navigate to the Symantec Data Loss Prevention keystore directory.
- 2 Enter the following command:

UninstallPwdKeyGenerator.exe -xp=<uninstall password>

where <uninstall password> is the password that you want to use. Choose a unique password key.

A password key is generated. Enter this key in the command line when you install the agent.

# Starting DLP Agents that run on Mac endpoints

You can use the start agent tool to start DLP Agents that run on Mac endpoints. You use the tool if the agents have been shut down using the shutdown task on the Agent List screen.

This tool is available in the AgentInstaller Mac64.zip file. This file is created after you complete the agent installation package process.

See "Generating agent installation packages" in the Symantec Data Loss Prevention Installation guide for more information.

Note: You must unzip this file to a Mac endpoint. You cannot use the tool if it is unzipped to a Windows endpoint.

#### To start agents using the start\_agent tool:

From the Symantec Data Loss Prevention Agent installation directory, run the following command:

```
start agent
```

where the installation directory is the directory where you installed Symantec Data Loss Prevention.

Go to the **Agent List** screen and confirm that the agent is running.

See "Using the Agent List screen" on page 1460.

See "About Endpoint tools" on page 1523.

10

# Section

# Monitoring and preventing data loss on mobile devices

- Chapter 79. Introducing Symantec Data Loss Prevention Mobile Prevent for Web
- Chapter 80. Implementing Mobile Prevent for Web

# Introducing Symantec Data Loss Prevention Mobile Prevent for Web

This chapter includes the following topics:

- How Mobile Prevent for Web works
- About deploying Mobile Prevent for Web
- About digital certificates for Mobile Prevent for Web
- About the VPN server and VPN On Demand
- About Microsoft Exchange ActiveSync and Mobile Prevent for Web
- About mobile device management

#### How Mobile Prevent for Web works

Mobile Prevent for Web connects to your corporate network through Wi-Fi access or through cellular 3G connectivity. Network traffic for Webmail, third-party applications such as Yahoo and Facebook, and corporate email applications including Microsoft Exchange ActiveSync, is sent through the HTTP/S protocol. Corporate email can be sent through Microsoft ActiveSync as either HTTP or HTTPS protocol information. Microsoft ActiveSync receives the information from the corporate proxy server after it has gone through detection; then, sends the message to the corporate Exchange Server. Messages that are sent through applications such as Facebook or Dropbox can be blocked from the message, depending on your policies.

See "About deploying Mobile Prevent for Web" on page 1535.

Mobile devices must connect to the corporate network through a virtual private network (VPN) to send corporate messages or access the corporate network. The Mobile Prevent for Web solution requires that mobile devices use the VPN On Demand feature to create a constant, protected VPN connection. If you are not connected to the corporate network, Mobile Prevent for Web cannot detect any policy violations.

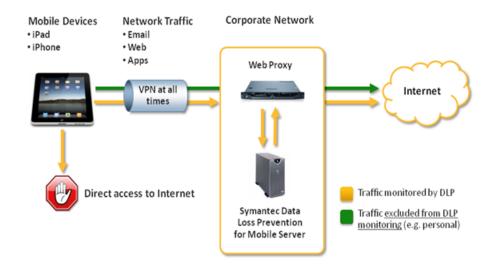
See "About the VPN server and VPN On Demand" on page 1538.

VPN configuration can be specified in a configuration profile by your mobile device management (MDM) solution. The MDM solution applies a configuration profile to each mobile device that you want to connect to your corporate network.

See "About mobile device management" on page 1541.

See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for details about requirements for Mobile Prevent for Web.

The following graphic illustrates the connections necessary to enable Mobile Prevent for Web:

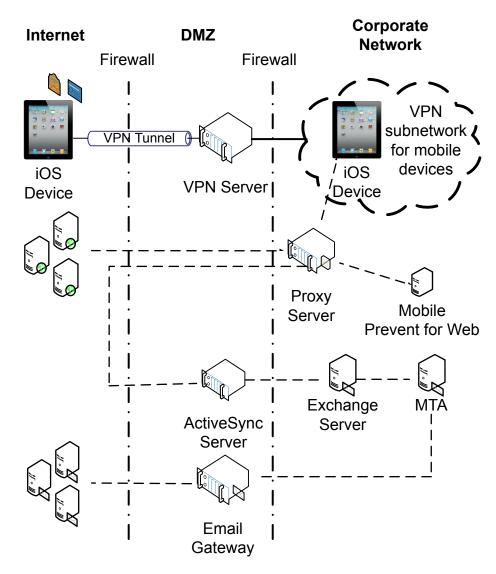


See "Implementing Mobile Prevent for Web" on page 1542.

# **About deploying Mobile Prevent for Web**

The Mobile Prevent for Web Server interacts with the Enforce Server and the corporate proxy server to monitor and prevent incidents on mobile devices.

The following diagram describes how the Mobile Prevent for Web solution fits into your corporate infrastructure:



In this deployment, mobile devices connect to the corporate network through your VPN server. The VPN server assigns each mobile device an IP address. This address lets the device access the internal corporate network. After the device is assigned a unique IP address, all HTTP, HTTPS, and FTP traffic is monitored by the Mobile Prevent for Web Server. Each device must be connected to the corporate network through the VPN. If the VPN connection to the corporate network is lost, Mobile Prevent for Web cannot detect any violations.

iPads and iPhones use a native feature called VPN On Demand to create a secure VPN connection automatically without user intervention. VPN On Demand requires certificate-based authentication to create the connection to the VPN Server.

After the VPN connection is established, traffic is sent through the proxy server and analyzed by Mobile Prevent for Web Server. Traffic between the proxy server and the Mobile Prevent for Web Server is done over the ICAP protocol. If no violations are discovered, the traffic is sent to its destination either internally or externally. If violations are discovered, an incident is created and response actions are implemented. Incidents are recorded on the Enforce Server.

When a mobile device sends an email through Microsoft Exchange ActiveSync. the HTTP/HTTPS packets are sent to the ActiveSync server. The packets are then sent to the Exchange Server. Any corporate email should go through Microsoft Exchange ActiveSync. Mobile Prevent for Web does not support the SMTP protocol.

Note: Mobile Prevent for Web does not support response mode (RESPMOD).

# About digital certificates for Mobile Prevent for Web

Mobile Prevent for Web requires digital certificates to ensure the validity of the user, enable certificate-based authentication to the VPN server, and allow SSL interception by the proxy server.

See "About authenticating users" on page 85.

You can use an MDM solution to deploy the certificates to multiple mobile devices as part of the mobile device profile.

See "About mobile device management" on page 1541.

See "Configuring the VPN profile" on page 1547.

The following table describes the four certificates that you must create for Mobile Prevent for Web:

Digital certificates for Mobile Prevent for Web **Table 79-1** 

Certificate	Where installed	Description
Certificate Authority (CA) root certificate	mobile devices, VPN Server, proxy server	The base CA. All other certificates are signed by the root CA or its subordinate CA. If a device trusts the root CA, then it trusts all valid certificates that are signed by the root CA or the subordinate CA.

Digital Certificates for Mobile Prevent for Web (continued)		
Certificate	Where installed	Description
User certificate	mobile devices	Identifies individual users. Users must have this certificate to gain access to the corporate subnetwork. The certificate is sent to the VPN server for authentication. This certificate is required to establish the VPN tunnel to the corporate network.
Subordinate certificate authority	Proxy server	The subordinate CA certificate grants the proxy server the permission to issue server identity certificates for HTTPS servers. This certificate is needed for SSL interception. After the mobile device has connected to the corporate subnetwork, the proxy server intercepts the traffic. The proxy server then acts as a go-between for the HTTPS server and the mobile device.
		The proxy server acts as a subordinate CA and verifies the certificate from the HTTPS server and issues a new certificate for the HTTPS server.
Device certificate	VPN Server	Establishes that the identity of the VPN server host name is valid before the mobile device can connect to it. The certificate ensures that the mobile device does not connect to an unauthorized VPN server.

Table 70-1 Digital certificates for Mobile Prevent for Web (continued)

## About the VPN server and VPN On Demand

Your mobile device connects to the VPN server to gain access to your corporate network.

The VPN server assigns an IP address to each mobile device that connects to it. These IP addresses form a VPN subnetwork. The VPN subnetwork lets your mobile devices access the corporate network and the corporate proxy server. You can specify a range of IP addresses that your VPN server can assign to other devices. All of the IP addresses that the VPN server assigns to your mobile devices are within this range. If a range of addresses were not specified for your VPN server. the network could randomly assign IP addresses to your mobile devices. A specific range of IP addresses lets Symantec Data Loss Prevention identify which IP addresses are assigned to mobile devices and which addresses are not connected. Using a range of IP addresses assists in identifying which mobile device generated an incident.

On the Mobile Prevent for Web side, VPN On Demand ensures that the VPN connection is not interrupted. Apple mobile devices use VPN On Demand to dynamically create a VPN session. VPN on Demand starts the VPN session when connecting to a specific list of configured domains (for example .com, .net, or .org). Certificate-based authentication is required to configure the VPN On Demand feature. By configuring how VPN On Demand automatically enables VPN on an iOS mobile device, you can ensure that all traffic goes through your corporate network. You need a Web proxy that is deployed in transparent mode to route traffic from the mobile devices in your corporate network to Symantec Data Loss Prevention. The network traffic is routed uses the ICAP service.

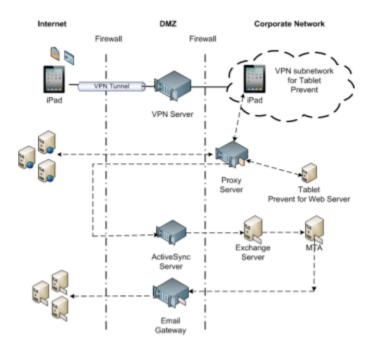
You can use a mobile device management (MDM) solution to apply the network and VPN configuration.

# About Microsoft Exchange ActiveSync and Mobile Prevent for Web

Microsoft Exchange ActiveSync is a way that you can send corporate emails from a mobile device. ActiveSync can send email either to recipients internal to the corporate network or outside of the corporate network. ActiveSync sends corporate email through an HTTP or HTTPS protocol. Any sensitive information transferring internally or externally that violates your policies is blocked.

The following diagram illustrates how corporate messages are sent through ActiveSync:

Note: The following diagram also applies to iPhones.



In this example, messages are sent from the iPad email client, which is configured with ActiveSync, through the VPN-connected corporate network. The message is sent as an HTTP/S request. The message is received in the ActiveSync Server and sent on to the Microsoft Exchange Server. The Exchange Server sends the message to the MTA server as an SMTP message. The MTA server sends the corporate message on to the recipient.

You can disable ActiveSync monitoring by filtering.

Note: Mobile Prevent for Web does not support blocking or redacting contacts and calendar traffic.

See "Ignoring Microsoft Exchange ActiveSync monitoring" on page 1540.

# Ignoring Microsoft Exchange ActiveSync monitoring

If you do not want to monitor corporate email messages going through ActiveSync, use the following procedure:

#### Ignoring Microsoft Exchange ActiveSync monitoring

- On the Enforce Server administration console, go to the Server Settings for the Mobile Prevent for Web Server.
- In the Request Filtering section, add the host name of the ActiveSync Server to the Ignore Requests to Hosts or Domains field.
- 3 Click Save.

See "About Microsoft Exchange ActiveSync and Mobile Prevent for Web" on page 1539.

# About mobile device management

Use a mobile device management (MDM) solution to manage and apply a wide variety of configuration settings to multiple mobile devices. You can load user profiles where corporate mail settings, VPN settings, security certificates, and proxy server settings are preconfigured onto the mobile devices. To access the Mobile Prevent for Web Server, you must use an MDM solution to apply the VPN server configuration profile. The VPN server configuration profile sets the conditions for VPN On Demand to route all network traffic through the VPN and into your corporate network. Only network traffic flowing in your corporate network can be monitored for violations.

See "Configuring the VPN profile" on page 1547.

# Implementing Mobile Prevent for Web

This chapter includes the following topics:

Implementing Mobile Prevent for Web

# Implementing Mobile Prevent for Web

The Mobile Prevent for Web Server integrates with a VPN server, an MDM solution, and a Web proxy server using ICAP. If it detects confidential data in Web content, the proxy will reject requests or remove HTML content as specified in your Mobile Prevent for Web policies.

First, you need to know the high-level steps that are required for implementing Mobile Prevent for Web. You can check the cross-referenced sections for more details. The following procedure assumes that you are implementing Mobile Prevent for Web as a standalone product.

See "About deploying Mobile Prevent for Web" on page 1535.

**Note:** These procedures assume that you already have your VPN and proxy servers running in your environment.

Table 80-1 Implementing Mobile Prevent for Web

Step	Procedure	For more information
Step 1	Add a new Mobile Prevent for Web Server.	See "Adding a detection server" on page 194.

Step	Procedure	For more information
Step 2	Configure your Mobile Prevent for Web Server.	See "Configuring the Mobile Prevent for Web Server" on page 1543.
Step 3	Configure your VPN Server with the IP address range that you want to assign to the corporate mobile devices for the Mobile Prevent for Web sub-network	See the documentation for your VPN Server.
Step 4	Configure your VPN profile with the MDM application.	See "Configuring the VPN profile" on page 1547.
Step 5	Define ICAP services on proxy to route traffic to Mobile Prevent for Web.	See "About proxy server configuration" on page 1170.
Step 6	Create and deploy a policy for Mobile Prevent for Web.	See "Creating policies for Mobile Prevent for Web" on page 1551.
Step 7	Test the system by generating an incident against your test policy.	See "Testing Mobile Prevent for Web" on page 1554.
Step 8	If required, troubleshoot the implementation.	

Table 80-1 Implementing Mobile Prevent for Web (continued)

See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for more details on configuring Mobile Prevent for Web to work within your organization.

# Configuring the Mobile Prevent for Web Server

You can use a number of configuration options for Mobile Prevent for Web Server. For example, you can configure the server to:

- Ignore small HTTP/S requests or responses.
- Ignore requests to or responses from a particular host or domain (such as the domain of a business subsidiary).
- Ignore user search engine queries.

See "Adding a detection server" on page 194.

#### To modify your Mobile Prevent for Web Server configuration

- 1 Go to System > Servers > Overview and click the Mobile Prevent for Web Server.
- 2 On the Server Detail screen that appears, click Configure.

You can verify or modify settings on the ICAP tab as described in subsequent steps. The tab is divided into several sections: Request Filtering, Response Filtering, and Connection.

- Verify or change the **Trial Mode** setting.
- 4 Verify or modify the filter options for requests from HTTP clients (user agents). The options in the **Request Filtering** section are as follows:

Ignore Requests Smaller Than	Specifies the minimum body size of HTTP
	requests to inspect. (The default is 4096
	bytes.) For example, search-strings typed
	in to search engines such as Yahoo or
	Google are usually short. By adjusting this
	value, you can exclude those searches
	from inspection.

#### Ignore Requests without Attachments Causes the server to inspect only the requests that contain attachments. This option can be useful if you are mainly concerned with requests intended to post

sensitive files.

Causes the server to ignore requests to the hosts or domains you specify. This option can be useful if you expect a lot of HTTP traffic between the domains of your corporate headquarters and branch offices. You can type one or more host or domain names (for example, www.company.com), each on its own line.

Causes the server to ignore requests from user agents (HTTP clients) you specify. This option can be useful if your

organization uses a program or language (such as Java) that makes frequent HTTP requests. You can type one or more user agent values (for example, java/6.0.29),

each on its own line

#### Ignore Requests to Hosts or Domains

#### Ignore Requests from User Agents

5

Note: The Response Filtering options are not supported for Mobile Prevent.

Verify or modify the filter options for responses from Web servers. The options in the Response Filtering section are as follows:

Ignore Responses Smaller Than

Specifies the minimum size of the body of HTTP responses that are inspected by this server. (Default is 4096 bytes.)

**Inspect Content Type** 

Specifies the MIME content types that Symantec Data Loss Prevention should monitor in responses. By default, this field contains content-type values for Microsoft Office, PDF, and plain text formats. To add others, type one MIME content type per

line. For example, type

application/wordperfect5.1 to have Symantec Data Loss Prevention analyze WordPerfect 5.1 files.

Note that it is generally more efficient to specify MIME content types at the Web

proxy level.

Ignore Responses from Hosts or **Domains** 

Causes the server to ignore responses from the hosts or domains you specify. You can type one or more host or domain names (for example, www.company.com),

each on its own line.

Ignore Responses to User Agents

Causes the server to ignore responses to user agents (HTTP clients) you specify. You can type one or more user agent values (for example, java/1.4.2 xx), each on its own line.

Verify or modify settings for the ICAP connection between the HTTP proxy server and the Mobile Prevent for Web Server. The Connection options are as follows:

TCP Port Specifies the TCP port number over which

> this server listens for ICAP requests. This number must match the value that is configured on the HTTP proxy that sends ICAP requests to this server. The

recommended value is 1344.

**Maximum Number of Requests** Specifies the maximum number of

> simultaneous ICAP request connections from the HTTP proxy or proxies. The

default is 25.

**Maximum Number of Responses** Specifies the maximum number of

> simultaneous ICAP response connections from the HTTP proxy or proxies. The

default is 25.

Connection Backlog Specifies the number of waiting

> connections allowed. A waiting connection is a user waiting for an HTTP response from the browser. The minimum value is 1. If the HTTP proxy gets too many requests (or responses), the proxy handles them according to your proxy configuration. You can configure the HTTP proxy to block any requests (or responses) greater than

this number

In the Mobile IP Ranges fields, enter the range of IP addresses that your VPN server is configured to assign to mobile devices. The IP addresses are used to identify the incidents that were triggered from mobile devices as Mobile incidents.

The IP addresses you enter into this range do not dynamically affect the VPN Server. This range is only to identify your mobile devices in the administration console. You must enter the exact same range of IP addresses when you configure the VPN Server to assign the addresses.

Click Save to exit the Configure Server screen and then click Done to exit the Server Detail screen.

# Configuring the VPN profile

You must configure the VPN profile before mobile devices can connect to the corporate network. The VPN profile combines security certificates, the VPN server configuration settings, VPN On Demand settings, and any network configuration settings. Normally, the VPN profile is set and applied through your MDM solution. Along with the VPN profile, you can configure other aspects of your mobile device such as Microsoft Exchange ActiveSync, firewall properties, or LDAP settings.

See "About mobile device management" on page 1541.

The following table describes the minimum VPN profile settings that you must make to enable Mobile Prevent. Depending on your MDM solution, the name of the setting may differ.

Table 80-2 Basic VPN profile settings

Type of setting	Setting	Description
VPN Configuration settings		
	Connection Name	The name of the connection type. Usually, this is a unique name so that you can identify it later.
	Connection Type	Select the connection type for your VPN server. For example, IPSec (Cisco).
	Server Name	Enter the host name or IP address for your VPN server.
	User Name	The user name for the mobile device that connects to the VPN server.  For example, <firstname_lastname> where the first name</firstname_lastname>
		and the last name of the user is specified.
	Machine Authentication	Select the certificate option. To enable Mobile Prevent for Web, you must use certificates for your company and your Certificate Authority.
	Identity Certificate	Select the certificate of the user you want to add.

		,
Type of setting	Setting	Description
	Enable VPN	You must enable VPN On Demand.
On Dema	On Demand	After you have enabled VPN On Demand, you can add the specific domain suffixes that you want. All domain suffixes should be enabled with the On Demand Action <b>Always Establish.</b>
		For example, the domain suffixes .com, .netorg, and .gov are added as <b>Always Establish</b> . Any time a domain name with one of those suffixes is called, the VPN tunnel must be established before the connection can complete.
Credential Settings		
	My Company	The certificate for your company. This is the root certificate for the Certificate Authority (CA).
	Our Company	This is the certificate for the proxy server.
	User Credential	This is the individual user certificate to access the proxy server.
Wi-Fi Settings		Use Wi-Fi settings if you want to mandate specific Wi-Fi networks wherein your mobile device will only work with specific networks. If you specify unique Wi-Fi settings, your mobile device cannot connect to any other Wi-Fi network.

**Table 80-2** Basic VPN profile settings (continued)

# About proxy server configuration for Mobile Prevent for Web

You must configure at least one HTTP/S proxy server to forward Web requests to Mobile Prevent for Web. The HTTP proxy acts as an ICAP client to the Mobile Prevent for Web Server. Mobile Prevent for Web supports only the request modification (REQMOD) mode of ICAP. Do not configure your HTTP proxy for the response modification (RESPMOD) mode.

Note: The proxy server must be deployed in transparent mode. Consult the proxy server documentation for details.

See "Specifying one or more proxy servers" on page 1173.

See "Proxy server compatibility with Mobile Prevent for Web" on page 1549.

See "Configuring the request mode service" on page 1549.

### Proxy server compatibility with Mobile Prevent for Web

Mobile Prevent for Web Servers can operate with the following Web proxies:

Mobile Prevent for Web supported proxy servers Table 80-3

Proxy	Supported protocols	Configuration information
•	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Blue Coat product documentation

See "Specifying one or more proxy servers" on page 1173.

See "About proxy server configuration" on page 1170.

### Configuring the request mode service

For details on configuring the proxy server, refer to your proxy server product documentation, or contact your proxy server administrator.

### To configure a proxy server:

REQMOD. On your proxy server, create an ICAP REQMOD service that forwards requests to Mobile Prevent. If your proxy server supports different protocols, configure it to handle the desired protocols.

For REQMOD mode, an ICAP service on the proxy server should look like:

```
icap://ip address|FQDN[:port]/reqmod
```

#### Where:

- ip address|FQDN identifies the Mobile Prevent for Web Server using either an IP address or fully qualified domain name.
- Port is the port number to which the Mobile Prevent for Web Server listens. Specifying the port number is optional when the default ICAP port (1344) is used.
- /reqmod is required for correct functionality in REQMOD mode.

### Examples:

```
icap://10.66.194.45/regmod
icap://10.66.194.45:1344/reqmod
icap://netmonitorl.company.com/reqmod
```

Note: The port that is specified in the ICAP service definition on the proxy must match the port where Mobile Prevent for Web Server listens.

See "About proxy server configuration" on page 1170.

# Specifying one or more proxy servers

By default, Mobile Prevent for Web Server can accept connections to the ICAP service port from any system on the network. For security reasons, you can limit ICAP connections to only those systems that you designate (or "whitelist"). Once you whitelist one or more systems, systems not on the whitelist cannot connect to the Mobile Prevent for Web Server ICAP service port.

Note: A proxy server whitelist can be affected by the **lcap.BindAddress** setting. By default, the **Icap.BindAddress** setting is 0.0.0.0, and the listener binds to all available addresses. If the Icap.BindAddress instructs the listener to bind to a specific IP, a whitelisted proxy must also be able to reach the listener address.

To create a whitelist of systems allowed to make a connection to the Mobile Prevent for Web Server ICAP service port:

- In the Enforce Server administration console, go to System > Servers > Overview and click the desired Mobile Prevent for Web Server.
- 2 On the **Server Detail** screen that appears, click **Server Settings**.
- 3 Scroll down to the **lcap.AllowHosts** setting.
  - By default, Icap.AllowHosts is set to any, meaning that all other systems on the network can communicate with this Mobile Prevent for Web Server.
- You can limit the systems that are allowed to connect with this Mobile Prevent for Web Server. Delete any and enter the IP addresses or Fully-Qualified Domain Name (FQDN) of the systems you want to authorize.
  - Separate multiple addresses with commas. For example: 123.14.251.31, webcache.corp.mycompany.com, 123.14.223.111. Use only commas to separate multiple entries; do not include spaces.
- 5 Click Save.

Changes to this setting do not take effect until you restart the Mobile Prevent for Web Server.

See "Proxy server compatibility with Mobile Prevent for Web" on page 1549.

See "About proxy server configuration for Mobile Prevent for Web" on page 1548.

### Enabling GET processing for Mobile Prevent for Web

By default, Mobile Prevent for Web does not process HTTP GET commands because of the high traffic volume. Follow this procedure to enable the server to process GET commands:

### To enable GET processing with Mobile Prevent for Web

- Configure the Web proxy server to forward GET requests to the Mobile Prevent for Web Server as described in your proxy server documentation.
- Ensure that the L7.processGets Advanced Server setting on the Mobile Prevent for Web Server must be "true" (which is the default).
- 3 Reduce the size of the L7.minSizeofGetURL Advanced setting on the Mobile Prevent for Web Server. Reduce from the default of 100 to a number of bytes smaller than the length of the shortest Web site URL from which you want to process GET commands. A minimum URL size to 10 should cover all cases. Note, however, that reducing the minimum size of GETs increases the number of requests that have to be processed, which increases the server traffic load.
- 4 Adjust the Ignore Requests Smaller Than setting in the ICAP section of the Mobile Prevent for Web Server Detail page. Reduce it from the default of 4096 bytes to a lower value that would enable the request to undergo DLP inspection. Note, however, that lowering the value increases the server traffic load.

# Creating policies for Mobile Prevent for Web

You can create the policies that include most standard response rules. The response rules include Add Note, Limit Incident Data Retention, Log to a Syslog Server, Set Attribute, and Set Status.

See "About Symantec Data Loss Prevention reports" on page 1006.

You can also incorporate the response rules that are specific to Mobile Prevent for Web as follows:

#### Mobile Prevent for Web: Block HTTP/HTTPS

Blocks the posts that contain confidential data (as defined in your policies). This includes Web postings, Web-based email messages, and files that are uploaded to Web sites or attached to Web-based email messages.

Note: Certain applications may not provide an adequate response to the Mobile Prevent for Web: Block HTTP/HTTPS response action. This behavior has been observed with the Yahoo! Mail application when a detection server blocks a file upload. If a user tries to upload an email attachment and the attachment triggers a Mobile Prevent for Web: Block HTTP/HTTPS response action, Yahoo! Mail does not respond or display an error message to indicate that the file is blocked. Instead, Yahoo! Mail appears to continue uploading the selected file, but the upload never completes. The user must manually cancel the upload at some point by pressing Cancel.

Other applications may also exhibit this behavior, depending on how they handle the block request. In these cases a detection server incident is created and the file upload is blocked even though the application provides no such indication.

### Mobile Prevent for Web: Remove HTTP/HTTPS Content

Removes confidential data from posts that contain confidential data (as defined in your policies). This includes Web-based email messages and files that are uploaded to Web sites. Note that the Remove HTTP/HTTPS Content action works only on requests.

■ Mobile Prevent for Web: Block FTP Request Blocks FTP transfers that contain confidential data (as defined in your policies).

For details on setting up any response rule action, open the online Help.

Go to Manage > Policies > Response Rules and click Add Response Rule.

Even if you do not incorporate response rules into your policy, Mobile Prevent captures incidents as long as your policies contain detection rules. You can set up such policies to monitor Web and FTP activity on your mobile device before implementing the policies that block or remove content.

If you have configured your proxy to forward both HTTP/HTTPS requests and responses, your policies work on both. For example, policies are applied to both an upload to a Web site and a download from a Web site.

### To create a test policy for Mobile Prevent for Web

- In the Enforce Server administration console, create a response rule that includes one of the actions specific to Mobile Prevent. For example, create a response rule that includes the Mobile Prevent for Web: Block HTTP/HTTPS action.
  - See "Configuring response rules" on page 891.
- 2 Create a policy that incorporates the response rule you configured in the previous step.

For example, create a policy called Test Policy as follows:

- Include a Content Matches Keyword detection rule that matches on the keyword "secret."
- Include a Mobile Prevent for Web: Block HTTP/HTTPS response rule.
- Associate it with the Default policy group.

See "Configuring policies" on page 326.

# Configuring Mobile Prevent for Web for secure banking

To enable mobile device users to send their own banking information, you can configure the proxy server to allow such traffic to bypass detection servers. Bypassing the detection servers allows mobile device users to access and use their own personal credit card and online banking information for legitimate purposes. If the proxy server is not configured to allow personal banking information to bypass detection, users might create incidents by submitting personal banking information. Symantec Data Loss Prevention users with relevant role-based privileges can potentially view the incident snapshots that contain confidential banking information of users within your organization.

Configure the proxy server to redirect network traffic directly to banking Web sites. This solution can also be used to allow network traffic to other secure Web sites. By redirecting the traffic to these specific Web sites, mobile device users can access these sites without generating false policy violations. The information that they send to these sites is not viewable by others in your organization.

Note: The following procedure is an example of how to configure a Blue Coat proxy server to redirect network traffic. For more information on configuring a proxy server, see the documentation that comes with the proxy server.

### Configuring the proxy server to redirect network traffic

- 1 Log in to the proxy server using an administrator account.
- 2 Open Visual Policy Manager (VPM).
- 3 Select SSL Intercept Layer policy.
- Add a rule for the destination host. For this example, enter the host name of the banking Web site that users are allowed to access.
- 5 Under Action, select Disable SSL interception.
- 6 Click **Apply** to save the changes.

# Testing Mobile Prevent for Web

You can test Mobile Prevent for Web by sending an email that violates your test policy.

### To test your system

- Connect your mobile device to the Internet and connect to your corporate VPN.
- 2 Open your corporate email client and send an email with an attachment containing confidential data. For example, access your Microsoft Outlook client and send an email with an attachment containing the word secret and paragraphs of other text.
- In the Enforce Server administration console, go to Incidents > Mobile and click Incidents - All. Look for the resulting incident. For example, search for an incident entry that includes the appropriate timestamp and policy name.
- 4 Click the relevant incident entry to see the complete incident snapshot. See "About strategies for using reports" on page 1007.

111

# Section

# Monitoring data loss from corporate emails downloaded to mobile devices

- Chapter 81. Introducing Symantec Data Loss Prevention Mobile Email Monitor
- Chapter 82. Implementing Symantec Data Loss Prevention Mobile Email Monitor

# Introducing Symantec Data Loss Prevention Mobile Email Monitor

This chapter includes the following topics:

- About Mobile Email Monitor
- How Mobile Email Monitor works
- Using Mobile Email Monitor with Mobile Prevent for Web

# **About Mobile Email Monitor**

More and more employees bring their own devices to work. With these personal devices, employees also bring the ability to download confidential corporate information. Mobile Email Monitor provides you with the ability to monitor your company's confidential information when it is sent from your corporate network to these personal devices; for example, to the native email client on iPads, iPhones, and other supported mobile devices.

While Mobile Email Monitor doesn't block this data, it does give you insight into what confidential data is downloaded. Mobile Email Monitor provides the data to the Enforce Server. With the Enforce Server administration console, you can create reports that continuously create a record of sensitive information that is downloaded to mobile devices. If the devices are lost or stolen, you can identify what downloaded emails left your corporation with these devices.

You can use the information that Mobile Email Monitor provides you about downloaded content to define mobile security policies for your corporation. Mobile Email Monitor can support your company's Bring Your Own Device (BYOD) policy

because it does not require installation of any applications or components on personal mobile devices. In addition, Mobile Email Monitor does not inspect information generated by personal applications installed on mobile devices.

See "How Mobile Email Monitor works" on page 1557.

# How Mobile Email Monitor works

Mobile Email Monitor inspects corporate emails that are sent to mobile devices through Microsoft Exchange Active Sync, using a reverse proxy. Unlike Symantec Data Loss Prevention Mobile Prevent for Web, Mobile Email Monitor does not require a VPN.

See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for more details about requirements for Mobile Email Monitor.

Figure 81-1 gives a graphical overview of how an email travels to a mobile device when you are using Mobile Email Monitor.

Symantec Data Loss Prevention Mobile Email Monitor Overview Figure 81-1

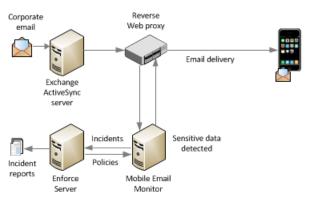


Table 81-1 provides more detail about how an email destined for download to a mobile device is monitored.

Table 81-1 Monitoring an email destined for a mobile device

Step	Action
Step 1	An email is downloaded from the Exchange ActiveSync Server, using either the HTTP or HTTPS protocol, through a corporate reverse Web proxy using ICAP.
Step 2	A reverse Web proxy server intercepts the email and diverts it to Mobile Email Monitor for detection using ICAP.

Step	Action
Step 3	Mobile Email Monitor scans the email according to policies you have set up using the Enforce Server administration console.
Step 4	If the email violates a policy, an incident is logged in the Enforce Server.
Step 5	After inspection by Symantec Data Loss Prevention the email (ICAP response) is sent back to the Web proxy.
Step 6	The Proxy server then sends the email to the recipient mobile email client.

**Table 81-1** Monitoring an email destined for a mobile device (continued)

See "Using Mobile Email Monitor with Mobile Prevent for Web" on page 1558.

# **Using Mobile Email Monitor with Mobile Prevent for** Web

You can deploy Mobile Email Monitor as a standalone product or as an additional server in your existing Symantec Data Loss Prevention environment. License keys for both the Mobile Email Monitor Server and the Mobile Prevent for Web Server are included in the Symantec Data Loss Prevention for Mobile product.

See "Symantec Data Loss Prevention Mobile Email Monitor set up overview" on page 1559.

# Implementing Symantec Data Loss Prevention Mobile Email Monitor

This chapter includes the following topics:

- Symantec Data Loss Prevention Mobile Email Monitor set up overview
- Adding and configuring the Mobile Email Monitor Server
- About proxy server configuration
- Specifying one or more proxy servers
- Configuring the response mode service
- About digital certificates for Mobile Email Monitor
- Setting up native email clients for monitoring
- Creating policies for Mobile Email Monitor
- Testing Symantec Data Loss Prevention Mobile Email Monitor
- Troubleshooting Mobile Email Monitor Server

# Symantec Data Loss Prevention Mobile Email Monitor set up overview

Table 82-1 outlines the steps that are required for implementing Symantec Data Loss Prevention Mobile Email Monitor. The table contains cross-references to topics in this chapter, as well as to topics in the *Symantec Data Loss Prevention* 

Administration Guide. You must have a deployed Symantec Data Loss Prevention Enforce Server and have a working Microsoft Exchange ActiveSync Server up and running in your datacenter before implementing Mobile Email Monitor according to the steps in the table.

**Table 82-1** Implementing Mobile Email Monitor

Step	Procedure	For more information
Step 1	Add and configure a new Mobile Email Monitor Server.	See "Adding and configuring the Mobile Email Monitor Server" on page 1560.
		See "Adding a detection server" on page 194.
Step 2	Configure a proxy server.	See "About proxy server configuration" on page 1562.
		See the proxy server product documentation for more details.
Step 3	Specify one or more proxy servers	See "Specifying one or more proxy servers" on page 1562.
	and define ICAP services on the proxy to route traffic to the Mobile Email Monitor Server.	See the <i>Symantec Data Loss Prevention Administration Guide</i> for more information.
Step 4	Configure the response mode service.	See "Configuring the response mode service" on page 1563.
Step 5	Set up a digital certificate for communication with the proxy server.	See "About digital certificates for Mobile Email Monitor" on page 1564.
Step 6	Configure native mobile email	See "Setting up native email clients for monitoring" on page 1564.
	accounts to point to the proxy server.	See the documentation for your native mobile email clients.
Step 7	Create and deploy a policy for	See "Creating policies for Mobile Email Monitor" on page 1564.
	Mobile Email Monitor.	See the Symantec Data Loss Prevention Administration Guide for more information.
Step 8	Test the system by generating an incident against your test policy.	See "Testing Symantec Data Loss Prevention Mobile Email Monitor" on page 1565.

See "Adding and configuring the Mobile Email Monitor Server" on page 1560.

# Adding and configuring the Mobile Email Monitor Server

Here are some configuration options for the Mobile Email Monitor Server.

- Ignore small HTTP/S responses.
- Ignore responses from a particular host or domain (such as the domain of a business subsidiary).

### To modify your Mobile Email Monitor Server configuration

- Go to System > Servers > Overview and click the name of a Mobile Email Monitor Server.
- 2 On the **Server Detail** screen that appears, click **Configure**.

You can verify or modify settings on the ICAP tab as described in subsequent steps. The tab is divided into sections: Response Filtering and Connection.

3 Verify or modify the filter options for responses from email servers. The options in the **Response Filtering** section are as follows:

Ignore Responses Smaller Than	Specifies the minimum size of the body of
	HTTP responses inspected by this server.
	(The default is 4096 bytes.)

### **Inspect Content Type**

Specifies the MIME content types that Symantec Data Loss Prevention should monitor in responses. By default, this field contains content-type values for Microsoft Office, PDF, and plain-text formats. To add others, type one MIME content type per

line. For example, type

application/wordperfect5.1 to have Symantec Data Loss Prevention analyze WordPerfect 5.1 files.

Note that it is generally more efficient to specify MIME content types at the Web proxy level.

### Ignore Responses from Hosts or **Domains**

Causes the server to ignore responses from the hosts or domains you specify. You can type one or more host or domain names (for example, www.company.com), each on its own line.

### Ignore Responses to User Agents

Causes the server to ignore responses to user agents (HTTP clients) you specify. You can type one or more user agent values (for example, java/1.4.2 xx), each on its own line.

Verify or modify settings for the ICAP connection between the HTTP proxy server and the Mobile Email Monitor Server. The Connection options are as follows:

TCP Port The default is 1344.

**Maximum Number of Responses** Specifies the maximum number of

> simultaneous ICAP response connections from the HTTP proxy or proxies. The

default is 16.

Connection Backlog Specifies the number of waiting

> connections allowed. A waiting connection is a user waiting for an HTTP response. The default value is 16; the minimum value

is 1

Click Save to exit the Configure Server screen and then click Done to exit the Server Detail screen.

See "About proxy server configuration" on page 1562.

# About proxy server configuration

See Symantec Data Loss Prevention System Requirements and Compatibility Guide for information on proxy servers tested to operate with Mobile Email Monitor. See the proxy product documentation for more details on setting up the proxy.

You must configure at least one HTTP/S proxy server to relay email responses to Mobile Email Monitor. The HTTP proxy acts as an ICAP client to the Mobile Email Monitor Server. The proxy should be configured in response modification (RESPMOD) mode to relay email messages for inspection. Mobile Email Monitor supports only the response modification (RESPMOD) mode of ICAP. Do not configure your HTTP proxy for the request modification (REQMOD) mode.

See "Specifying one or more proxy servers" on page 1562.

# Specifying one or more proxy servers

By default, Mobile Email Monitor Server can accept connections to the ICAP service port from any system on the network. For security reasons, you can limit ICAP connections to only those systems that you designate (or "white list"). Once you white list one or more systems, systems not on the whitelist cannot connect to the Mobile Email Monitor ICAP service port.

Note: The Icap.BindAddress setting can affect a proxy server whitelist. By default, the Icap.BindAddress setting is 0.0.0.0, and the listener binds to all available addresses. If the Icap.BindAddress instructs the listener to bind to a specific IP, a whitelisted proxy must also be able to reach the listener address.

To create a whitelist of systems allowed to make a connection to the Mobile Email Monitor Server ICAP service port:

- In the Enforce Server administration console, go to System > Servers > Overview and click the desired Mobile Fmail Monitor Server.
- On the **Server Detail** screen that appears, click **Server Settings**.
- Scroll down to the **Icap.AllowHosts** setting.
  - By default, Icap.AllowHosts is set to any, meaning that all other systems on the network can communicate with this Mobile Email Monitor Server.
- You can limit the systems that are allowed to connect with Mobile Email Monitor. Delete any and enter the IP addresses or Fully-Qualified Domain Name (FQDN) of the systems you want to authorize.

Separate multiple addresses with commas. For example: **123.14.251.31,webcache.corp.mycompany.com,123.14.223.111**. Use only commas to separate multiple entries; do not include spaces.

Click Save.

Changes to this setting do not take effect until you restart the Mobile Email Monitor Server.

See the Symantec Data Loss Prevention System Requirements and Compatibility Guide for more details about supported proxy servers for Mobile Email Monitor.

See "Configuring the response mode service" on page 1563.

# Configuring the response mode service

For details on configuring the proxy server, refer to your proxy server product documentation, or contact your proxy server administrator.

### To configure a proxy server:

On your proxy server, create an ICAP RESPMOD service that forwards responses to Mobile Email Monitor. If your proxy server supports different protocols, configure it to handle the desired protocols.

For RESPMOD mode, an ICAP service on the proxy server should look like:

#### Where:

- ip\_address|FQDN identifies the Mobile Email Monitor Server using either an IP address or fully-qualified domain name.
- Port is the port number where Mobile Email Monitor listens. FQDN Specifying the port number is optional when the default ICAP port (1344) is used.
- /respmod is required for correct functionality in RESPMOD mode.

### Examples:

```
icap://10.66.194.45/respmod
icap://10.66.194.45:1344/respmod
icap://netmonitorl.company.com/respmod
```

Note: The port that is specified in the ICAP service definition on the proxy must match the port where Mobile Email Monitor Server listens.

See "About digital certificates for Mobile Email Monitor" on page 1564.

# About digital certificates for Mobile Email Monitor

The proxy server requires a digital certificate to communicate with mobile devices and the Exchange Server. See your proxy product documentation for more information.

See "Setting up native email clients for monitoring" on page 1564.

# Setting up native email clients for monitoring

Native email accounts from your user's devices should point to the reverse proxy that routes email to Mobile Email Monitor for Symantec Data Loss Prevention inspection. See the documentation for your native email clients for more information on setting up the email clients so that they point to the proxy.

See "Creating policies for Mobile Email Monitor" on page 1564.

See "How Mobile Email Monitor works" on page 1557.

# Creating policies for Mobile Email Monitor

Mobile Email Monitor only monitors email traffic to mobile devices, so no Prevent response rules will function with Mobile Email Monitor. You can create policies that include some standard rules. Mobile Email Monitor only monitors incidents, so you don't need response rules, as long as your policies contain detection rules. You can set up detection policies to monitor the emails downloaded to mobile devices.

### To create a test policy for Mobile Email Monitor

Create a policy that incorporates a standard test detection rule.

For example, create a policy called Test Policy as follows:

- Include a Content Matches Keyword detection rule that matches on the keyword "secret."
- Associate it with the Default policy group.

See "Testing Symantec Data Loss Prevention Mobile Email Monitor" on page 1565.

# Testing Symantec Data Loss Prevention Mobile Email Monitor

You can test Mobile Email Monitor by sending an email that violates your test policy.

### To test your system

- Send an email with an attachment containing the word secret and paragraphs of other text to your Microsoft Outlook email account.
- 2 Download the email using your mobile device.
- In the Enforce Server administration console, go to Incidents > Mobile Email **Monitor** and click **Incidents - All**. Look for the resulting incident. For example, search for an incident entry that includes the appropriate timestamp and policy name.
- Click the relevant incident entry to see the complete incident snapshot.

Note: Incident representation is OS dependent and thus will vary depending on the OS and device you are using.

See "Troubleshooting Mobile Email Monitor Server" on page 1565.

# **Troubleshooting Mobile Email Monitor Server**

Troubleshooting Mobile Email Monitor Server describes common problems you may encounter when you are using Mobile Email Monitor and suggests possible solutions.

**Table 82-2** Troubleshooting Mobile Email Monitor Server

Problem	Explanation or Possible Solution
Incidents do not appear in Symantec Data Loss Prevention Mobile reports.	The Ignore Responses Smaller Than parameter can cause emails smaller than the set parameter size to be ignored. To enable monitoring of smaller emails, set the parameter to a lower value.
An email preview feature can cause a single policy violation in an email to generate duplicate incidents.	If the email preview contains data that triggers a policy, Mobile Email Monitor will count the preview data as one incident and the same data in the body as another incident, for a total of two incidents.

# Index

Symbols	agent group
1066	conditions 1452
	Agent Groups 1443
A	deployment process 1445
• •	deployment strategy 1444
about	migration of existing Endpoint Servers 1446
incident details 978	agent groups
reports 977	assigning configurations to deploy 1454
VPN server 1538	creating a new 1453
access control lists (ACL)	updating outdated 1453
incident snapshots 1044	viewing and managing 1451
Active Directory 1447	Agent Host Domain 1447
attribute 1448	Agent Host Name 1447
attributes 1444	Agent Host Type 1447
AddDefaultHeader field 1158	Agent Host Version 1447
AddDefaultPassHeader field 1159	agent overview
administration	summary screen 1457
introduction to 55	alerts. See system alerts
administration console	AllowHosts field 1161, 1173, 1550, 1563
about 56	application monitoring 1374
logging on and off 57	about 1503
Administrator account	adding an application 1506
about 58	archive
email account 60	incidents 1065
password, changing 59	archived incidents
password, resetting 103	deleting 1068
AdminPasswordReset utility 103	restoring 1066
Advanced Process Control 177	archiving
advanced server settings 1148	incidents 1065–1066
Agent 1516	Attribute Query Resolver tool 1449
agent attribute	attribute values 1449
creating a new 1448	attributes 956, 961, 978, 986, 1078
agent attributes 1450	applying 1450
managing 1446	types 1448
user-defined 1451	user-defined 1447
Agent configuration	authentication credentials 131
about 1405	Authority Information Access field 118
adding 1406	, , , , , , , , , , , , , , , , , , ,
applying 1441	В
agent events	<del>_</del>
about 1490	banking
agent event detail screen 1492	Mobile Prevent for Web 1553

best practice	Classifying Enterprise Vault content
evaluate per-fold accuracy rates 538	Enabling test mode when 621
reject training if accuracy rate above 5% 538	clipboard 1373
best practices	code numbers
allocate low memory for endpoint policies 537	system events 150
collect as many example documents as	Common name (CN) values 117
possible 536	console. See administration console
create documents staging area 537	correlations 960, 985, 1003
do not use VML to detect graphics or PII 534	credential store
narrowly define the category 535	adding authentication 132
perform negative testing 528	deleting credentials 133
policies 357, 359–365	editing credentials 133
profiled DGM 665	endpoint credentials 132
seed the negative training set with generic	managing 133
content 536	credentials 131
tune profile before deploying into production 540	CRLDP revocation checks
undeploy unused profiles 540	configuring aproxy for 121
use documents archives 537	support for 118
use to detect unstructured, text-based	custom attributes 961, 986, 1076, 1078
content 533	creating 1079
VML, summary of 532	editing 1079
BindAddress field 1161, 1173, 1550, 1563	incident snapshots 1043
blocking requests 1175, 1551	Lookup option (incident snapshot) 1078
Blue Coat ProxySG 1171, 1549	populating 1078
BoxMonitor process 245	setting values manually 1080
Dominimon process 2 to	uses of 1078
C	using 1076
	•
CA certificates	D
importing 197	
CD/DVD	dashboard reports
about 1371	configuring 1014
Certificate authentication	creating 1012
adding CA certificates for 114	scheduling 1027
configuring 110	dashboards 1011
configuring revocation checks for 118, 120	deleting 1038
enabling or disabling 112	editing 1029
mapping CN values for 117	viewing 1012
troubleshooting 124	data classification
Certificate Revocation Lists Distribution Point. See	introduction 620
CRLDP revocation checks	Data classification services
checksum offloading 1143	incident list 1000
classification	incident snapshot 1001
incident list 1000	Data Identifiers
incident snapshot 1001	cloning, manually 565
classification events 621	modifying 551
Classification Server	Data identifiers
configuring 192	about 541
configuring retention categories for 917	best practices 579
Classification test mode 1000–1001	breadths, about 547

Data identifiers (continued)	detection (continued)
configuration, about 570	crackable text and markup formats 688
cross-component matching 548	crackable word-processing file formats 685
custom, about 572	Custom File Type Signature 617
data normalizers, about 578	file name 611, 614
extending 546	file name examples 615
optional validators, about 547	file name syntax 615
pattern language limitations, about 573	file properties 609
patterns 547	file size 611, 613
system-defined 542, 545	file type 609, 612
validators, about 548	file type, custom 610, 617
data identifiers	Message Attachment or File Name Match 614
adding 550	Message Attachment or File Size Match 613
breadths, list of 554	Message Attachment or File Type Match 612
Content Matches data identifier condition 552	mobile 627, 629
editing validator input 566	network 626, 628
implementing custom script validators 579	Protocol Monitoring, mobile 629
implementing, custom 570	Protocol Monitoring, network 628
implementing, patterns 574	word processing formats 684
managing 550	detection servers 277
normalizers, list of 555	about 177
optional validators, configuration 559	adding 194
optionl validators, acceptable characters 560	configuration 180
selecting validators 577	controls 178
data loss prevention. See Symantec Data Loss	errors and warning list 200
Prevention	kinds of 48
DBPasswordChanger utility	logging 251
example of using 279	removing 196
introducing 275, 279	Server Detail screen 201
locating 279	server settings 203
prerequisites for using 279	settings, advanced 193
running 279	single-tier 194
debug log files 243–244, 258	status of 198
delete	System Overview screen 198
archived incidents 1068	direcotry servers (LDAP)
deploying	configuring connections 127
SMS 1516	connecting to 126
using silent installation 1516	Directory Group Matching (DGM)
using the Endpoint FlexResponse utility 1518	implementing synchronized 656
detection	Recipient based on a Profiled Directory
best practice 618	condition 664
crackable CAD formats 690	Sender/User based on a Profiled Directory
crackable database file formats 690	condition 663
crackable email formats 689	synchronized 653
crackable encapsulation formats 691	Directory Group Matching (DGM), profiled
crackable graphics formats 690	profiled 661
crackable other formats 691	profiled conditions 663
crackable presentation formats 686	profiled conditions odd
crackable presentation formats 666 crackable spreadsheet formats 687	two-tier detection 661
S. S	

Directory Group Matching (DGM), profiled <i>(continued)</i> workflow 662	Endpoint Discover <i>(continued)</i> Endpoint Discover target 1389
Directory Group Matching (DGM), synchronized	how it works 1383
Recipient matches User Group based on a	implementing 1389
Directory Server Group 658	introducing 54
scheduling inexing 129	Max Scan Duration 1400
Sender/User matches User Group based on a	reports 1403
Directory Server Group 657	Scan Idle Timeout 1400
DLP agent	scan timeout settings 1400
health 1457	scanning 1383
DLP Agent summary reports 1467	target filters 1392
Legacy DLP Agents 1473	targeted scans 1385
document upload	Endpoint Discover scans
max size per 537	excluding items or repositories 1395
documents	including items or repositories 1395
supported types 537	Endpoint FlexResponse
Documentum targets 1339	about 1512
	deploying 1514
E	deploying plug-ins 1515
	deploying plug-ins using the Endpoint
ECU. See Environment Check Utility	FlexResponse utility 1518
eculogs.zip file	enabling on Enforce Servers 1519
contents of 278	uninstalling using the FlexResponse utility 1520
ECUoutput.txt file 278	Endpoint FlexResponse utility 1516
email	options 1517
blocking 1161	password 1518
quarantining 1163	endpoint incident
Endace cards 1145	destination or protocol specific information 974
configuring Network Monitor to use 1148	lists 964
drivers for 1146	snapshot 967
installing drivers for 1146	endpoint location
Endpoint 1000	setting 1378
Quarantine response rule 1388	Endpoint Prevent
user cancel response rule 1377	application monitoring 1374
endpoint 4444	block response rule 1375–1376
agent advanced settings 1414	CD/DVD monitors 1371
Agent log levels 1501	Citrix XenApp 1374
Agent logs 1500	Citrix XenDesktop 1374
incidnet summary screen 975	clipboard monitor 1373
incompatible detection and response rules 1366	creating policies 1375
policies for 1365	how it works 1367
response rules in different locales 1380	implementing 1378
setting response rules in different locales 1381	introducing 54
setting the endpoint location 1378	Microsoft Hyper-V 1374
summary reports 975	monitoring 1368
Endpoint Discover	network monitors 1369
adding a rule 1387	network share monitoring 1372
configuring targets 1390	notify response rule 1375–1376
creating a policy 1387	print/fax monitor 1372
creating a policy group 1386	

Remote Desktop Services 1374 removable media 1369 reporting response rules 972 reports 1403 virtual hosts 1374 virtual machines 1374 VMWare View 1374 Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce entroducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  example 367 exceptions 375 field mapping 374 functionality 368 index file 371 index updates 374 manage profiles 394 match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exact Data Matching (EDM), profile mapping fields 371  F filtering requests 1168, 1544 Firefox browser 994 ffirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on directions 375 field mapping 374 functionality 368 index file 371 index updates 374 manage profiles 394 match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exact Data Matching (EDM), profile mapping fields 389 schedule profi
reporting response rules 972 reports 1403 virtual hosts 1374 virtual machines 1374 VMWare View 1374  Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 277–278  field mapping 374 functionality 368 index file 371 index updates 374 manage profiles 394 match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 remote indexing 432 SQL Preindexer utility 433 two-tier detection 377 workflow 378  Exact Data Matching (EDM), configure Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
reports 1403 virtual hosts 1374 virtual machines 1374 VMWare View 1374 Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  forms-based log on  functionality 368 index file 371 index updates 374 manage profiles 394 match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 remote indexing 432 SQL Preindexer utility 433 remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
virtual hosts 1374 virtual machines 1374 VMWare View 1374 Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tolols 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1381 Enforce Server 277 Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–278 Index updates 374 manage profiles 394 match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
virtual machines 1374 VMWare View 1374  Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278
VMWare View 1374 Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 275–278  match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 remote indexing 432 SQL Preindexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378  Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Endpoint Server     configuration, basic 191     configuring file filters 1412 endpoint targets     configuring 1390 endpoint tools 1523     logdump.exe tool 1527     Service_Shutdown.exe tool 1525     using on Windows Vista 1525     vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce     introducing 50     logging 251 Enforce console. See administration console Enforce Server     about 56     alerts, configuring to send 146     choosing a non-English language for 70     enabling Endpoint FlexResponse 1519     introducing 50     response rules in different locales 1380     setting response rules in different locales 1381 Enforce Server administration console     Profile screen 60 Environment Check Utility     introducing 275–276     location 277–278 Enforce Server administration console     Profile screen 60 Environment Check Utility     introducing 275–276     location 277–278  match counting 413     policy condition 375     preparing for indexing 381     Remote EDM Indexer utility 433     two-tier detection 377     workflow 378     Exact Data Matching (EDM), configure     Exact Data Profile 385     Remote EDM Indexer utility 433     two-tier detection 377     workflow 378     Exact Data Matching (EDM), profile     mapping fields 389     schedule profile indexing 392     Exchange targets 1287     exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility     about 1516     deploying plug-ins 1518     retrieving plug-in list 1521     retrieving plug-ins 1520     uninstalling plug-ins 1520     uninstalling plug-ins 1520     forms-based log on
Endpoint Server configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1381 Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275-276 locating 277-278  match counting 413 policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 remote indexing 432 SQL Preindexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
configuration, basic 191 configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 location 272-278  policy condition 375 preparing for indexing 381 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffirst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
configuring file filters 1412 endpoint targets configuring 1390 endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 location 277–278 Possible 277 Encore Server administration console Profile screen 60 Environment Check Utility introducing 275–276 location 277–278 Encore Server administration console Environment Check Utility introducing 275–276 location 277–278 Encore Server administration console Environment Check Utility introducing 275–276 location 277–278 Encore Server administration console Environment Check Utility introducing 275–276 location 277–278 Encore Server administration console Environment Check Utility introducing 275–276 location 277–278 Encore Server administration console Environment Check Utility introducing 275–276 location 239 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Profile 385 Remote EDM Indexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  Friefox browser 994 frinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
endpoint targets
endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  SQL Preindexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
endpoint tools 1523 logdump.exe tool 1527 Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  SQL Preindexer utility 433 two-tier detection 377 workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Service_Shutdown.exe tool 1525 using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  workflow 378 Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  Friefox browser 994 flrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
using on Windows Vista 1525 vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 location 277–278  Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile Exact Data Matching (EDM), profile Exact Data Matching (EDM), profile Exact Data Matching (EDM), configure Exact Data Matching (EDM), configure Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), configure Exact Data Matching (EDM), configure Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  Friefox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
vontu_sqlite3.exe tool 1526 endpoint utilities 275 Enforce introducing 50 logging 251 Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Profile 385 Remote EDM Indexer 383 uploading the exact data source to Enforce 383 Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
endpoint utilities 275  Enforce introducing 50 logging 251  Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Remote EDM Indexer 383 uploading the exact data source to Enforce 383  Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 flirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Enforce introducing 50 logging 251  Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  uploading the exact data source to Enforce 383  Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
introducing 50 logging 251  Enforce console. See administration console Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Exact Data Matching (EDM), profile mapping fields 389 schedule profile indexing 392  Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
logging 251  Enforce console. See administration console  Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277  Enforce Server administration console Profile screen 60  Environment Check Utility introducing 275–276 locating 277–278  mapping fields 389 schedule profile indexing 392  Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Enforce console. See administration console  Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  schedule profile indexing 392 Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffirinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Enforce Server about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce Server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Exchange targets 1287 exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
about 56 alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  exporting agent attributes 1449  F filtering requests 1168, 1544 Firefox browser 994 flrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
alerts, configuring to send 146 choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  F  filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
choosing a non-English language for 70 enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  F filtering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
enabling Endpoint FlexResponse 1519 introducing 50 response rules in different locales 1380 setting response rules in different locales 1381 Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Intering requests 1168, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-ins 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
introducing 50 response rules in different locales 1380 setting response rules in different locales 1381  Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  Intering requests 1768, 1544 Firefox browser 994 ffrinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
response rules in different locales 1380 setting response rules in different locales 1381  Enforce server 277 Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278  File tox browser 994 firinst.exe utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
setting response rules in different locales 1381  Enforce server 277  Enforce Server administration console Profile screen 60  Environment Check Utility introducing 275–276  locating 277–278  Initiative utility about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Enforce server 277  Enforce Server administration console Profile screen 60  Environment Check Utility introducing 275–276  locating 277–278  about 1516 deploying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Enforce Server administration console Profile screen 60 Environment Check Utility introducing 275–276 locating 277–278 epiloying plug-ins 1518 retrieving plug-in list 1521 retrieving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
Profile screen 60 retrieving plug-in list 1521 Environment Check Utility introducing 275–276 retrieving plug-ins 1520 introducing 277–278 Forms-based log on
Environment Check Utility introducing 275–276 locating 277–278 Interving plug-ins 1520 uninstalling plug-ins 1520 Forms-based log on
introducing 275–276  locating 277–278  Forms-based log on
locating 277_278
output of 278
running 277–278 forwarding mode 1154–1155
EnvironmentCheckUtility command 277–278
ErrorLog.txt file 278
ethtool 1143 GET commands 1149, 1174, 1551
Exact Data Matching (EDM) group conflicts
add profiles 394 viewing 1455
creating the data source file 379 group exceptions, type
data source cleansing 373 Recipient Matches Pattern 648
data source size limits 372 group rules, type
Directory EDM 376 Recipient Matches Pattern 648
EDM condition 396

H	incident reports (continued)
Home page	sending by email 1041
selection 56	setting advanced filters 1056
HostFileLog.txt file 278	setting general filters 1047
HTTP proxies. See proxy servers	setting preferences 1008
HTTP requests 187	summaries 1011, 1016, 1046
blocking 1175, 1551	summary options 1040, 1051
ignoring 1167–1168, 1543–1544	viewing incidents 1018
HTTP responses	viewing summary reports 1016
ignoring 1561	incident snapshot
ig.io.iiig ioo.	classification 1001
I	incident snapshots
	ACL information 1044
ICAP 51, 1168, 1172–1173, 1544, 1549–1550, 1561–	correlations tab 1043
1563	custom attributes section 1043
configuring 1170, 1546, 1562	history tab 1042
incident details 978	matches section 1044
incident list	Network Discover 991
classification 1000	policy section 1043
incident lists	incident summaries
Mobile 978	Network Discover 999
Network Discover 995	Incident Update privilege 95
Network Monitor and Prevent 950	incidents 950, 955–957, 960–961, 978, 981, 983,
incident remediation 940	985–986
commands 945	archiving 1065–1066
email response variables 946	attributes, status 1069
Incident Reporting and Update API	custom attributes 1076
privileges 95	custom attributes, and 1079
Incident Reporting and Update Web Service 246	deleting 1034
Incident Reporting privilege 95	preventing archiving 1067
incident reports 1006	remediating 953, 980
creating summary reports 1017	restoring archived 1066
customizing 1019	incremental scanning 1222–1224
dashboards 1011, 1019	Indexed Docoument Matching
dashboards, configuring 1014	scheduling indexing 492
dashboards, creating 1012	Indexed Docoument Matching (IDM)
deleting custom reports 1038	adding document profiles 479
editing custom reports 1029	configuring document profiles 479
exporting to CSV 1029	configuring the match condition 497
exporting to XML 1029	excluding content using whitelisting 476
filter options 1040	filtering by file name 489
filtering 1021, 1046	filtering by file size 491
implementing a strategy 1007	implementing 475
introducing 1009	managing document profiles 477
navigating pages 1039	preparing the document source for indexing 475
Network Discover 990	Indexed Document Matching
printing 1042	DocSource.rdx 467
remediating incidents 943	EndpointDocSource.rdx 467
saving 1022	pointbooodiso.idx 101
scheduling 1023, 1025	

Indexed Document Matching (IDM)	logging (continued)
best practice 501, 503-506	per-fold evaluation rates 531
document data source 466	logging on and off 57
Document Profile 465	logs
exact file contents matching 471	review 149
exact file matching 470	lookup parameters
exception conditions 474	parameter groups 1096
IDM match condition 473	lookup plug-ins. See about
Overview 462	automatic lookup 1111
partial file contents matching 471	automatic reload 1111
Platforms 464	chaining 1108
remote indexing options 467	chaining multiple plug-ins 1097
whitelisting 474	CSV attribute mapping 1116
installation log files 243	CSV data file requirements 1114
installing	CSV file delimiter 1115
plug-ins 1516	CSV file location 1115
internationalization. See languages and character	CSV key mapping 1116
sets	CSV, character set 1116
Internet Content Adaptation Protocol. See ICAP	CSV, how it works 1094
iptables command 1159-1160	custom 1138
	custom (legacy) 1095
L	data owner email output 1111
<del>-</del>	data owner output 1111
Language Pack Utility 71	deployment 1097
language packs about 68	enabling 1107
Language Pack Utility 71	implementing, workflow for 1098
languages and character sets	LDAP attribute mapping 1123
character sets, using 67	LDAP configuration 1122
choosing a non-English language 70	LDAP server connection 1123
language packs, about 68	LDAP, how it works 1094
language packs, working with 71	lookup parameters 1102
legacy agent overview	reloading 1108
actions 1485	script chaining 1134
Legacy DLP Agent summary reports	timeout 1111
1473	types 1093
licenses 173	lookup plug-ins, script
Linux systems 1159	enabling credentials 1132
listing plugins 1516	encrypting credentials 1132
Livelink targets 1348	lookup plugin
localization. See languages and character sets	LDAP testing 1125
Lock Manager service 277	script protocol filtering 1131
log files 243	lookup plugins
logdump.exe tool 1527	script configuring 1127
logdump.exe utility 276	script writing 1128
Logged in User 1447	script, how it works 1094
Logged in User Domain 1447	scripting languages 1094
logging	Lotus Notes targets 1261
distance and confidence 531	

number of features modeled 531

M	Network Discover (continued)
mail transfer agents. See MTAs	editing targets 1189
manager process 245	how Discover works 1182
manager-certauth.security 123	how scanners work 1306
manager-certauth security file 121	incident lists 995
matches 960, 985	incident reports 988–990
Microsoft Exchange targets 1305	incident snapshots 991
Microsoft TMG 1171	incident summaries 999
MIME types 188, 1169, 1545, 1561	introducing 51, 1180
minSizeofGetURL field 1174, 1551	logging 248
Mobile Email Monitor 1562	quarantine files 1258
configuring proxy servers 1563	reports 988
configuring the response mode service 1563	setting up 1184
creating policies for 1564	Network Discover scans
introducing 53	auditing targets 1206
testing 1565	authentication 1196
troubleshooting 1565	deleting 1215
Mobile Email Monitor Server	differential scans 1225
adding 1560	encrypting passwords 1197
configuring 1560	excluding items or repositories 1198
Mobile Prevent	filtering by item size 1201
introducing 53	filtering by last-accessed date 1202
Mobile Prevent for Web	filtering by modified date 1202
banking 1553	including items or repositories 1198
configuring 1173, 1550	inventory scans 1206
creating policies for 1551	list of targets 1210
Deployment scenarios 1535	managing 1209
implementing 1542	monitoring 1209
testing 1554	optimizing 1204, 1220
troubleshooting 1177	parallel 1226
Mobile Prevent for Web Server	removing targets 1212
configuring 1543	reporting agen details, 1315
monitorSettings directory 277	reporting scan details 1215
monitorSettings folder 278	reporting scan history 1213 scheduling 1194
MTAResubmitPort field 1158	status 1219
MTAs 51, 186, 1152, 1154, 1157	throttling 1204
configuring 1160	Network Discover Server
MX records 185, 1156	configuration, basic 190
	configuring 1185
N	configuring parallel scans 1226
Napatech 1145	Linux 1187
Napatech cards	Network Discover targets 1315
configuring Network Monitor to use 1148	custom 1356
network connections	DB2 databases 1267
checking 277	Documentum 1339
Network Discover	Domino servers 1261
adding new targets 1187	Exchange 1287, 1305
configuring 1184	file shares 1241
configuring targets 1191, 1193	5.15.55

Network Discover targets (continued)	Network Protect
Livelink 1348	introducing 52
Lotus Notes 1261	quarantine files 1258
Oracle databases 1267	Network Protect server
removing 1212	configuration, basic 190
SharePoint 1274	network share monitoring 1372
SQL databases 1267	network taps 1141, 1144
SQL server 2005 1267	new_oracle_password parameter 279
UNIX file systems 1315	Next MTA field 1157
Web servers 1327	NIC 1142, 1145
Web services 1356	Notification service 277
Web sites 1327	
Windows remote server file systems 1315	0
network interface card. See NIC	
Network Monitor	OCSP revocation checks
configuring 1147	configuring 123
creating policies for 1150	configuring a proxy for 121
implementing 1141, 1143	disabling 123
introducing 51	support for 118
logging 250	Online Certificate Status Protocol. See OCSP
requirements for 1141	revocation checks
testing 1150–1151	operational log files 243
using Endace cards with 1147	Oracle database 277
Network Monitor Server	NLS_LANGUAGE setting 70
configuring 181	NLS_TERRITORY setting 70
Network Prevent (Email)	
bouncing messages 933	P
Network Prevent for Email	packet capture software 1142, 1144
blocking email 1161	installing 1145
configuring 1155	PACKET MMAP software 1145
creating policies for 1161	Password authentication
enabling policy violation headers 1163	disabling 125
implementing 1152, 1154	enabling or disabling 112
integrating MTAs with 1154	Password Renewal window 63
introducing 51	password_file parameter 279
logging 250	passwords 279
routing restricted ports to 1159	See also DBPasswordChanger utility
testing 1164	Administrator 59, 103
Network Prevent for Email Server	changing 60, 63, 279
configuring 184	encrypting for Network Discover scans 1197
Network Prevent for Web	resetting 103
	pcapstart.reg file 1146
configuring 1167	plug-ins
creating policies for 1175	deploying on the endpoint 1515
implementing 1165, 1167	Plugins.properties file 1232
introducing 51	
testing 1176	policies about 283
Network Prevent for Web Server	add 325
configuring 187	
	adding response rules 350

policies (continued) components 285	policy detection templates, configuration <i>(continued)</i> Employee Data Protection 815
configuration 326	Encrypted Data 817
create 345	EU Data Protection Directives 811
Data Profiles 291	Export Administration Regulations (EAR) 817
deployment 288	FACTA 2003 (Red Flag Rules) 818
manage 345	Financial Information 822
privileges, administration 290	Forbidden Websites 823
privileges, authoring 290	Gambling 824
privileges, response rules 290	Gramm-Leach-Bliley 824
removing 351	Human Rights Act 1998 830
solution pack 287	Illegal Drugs 831
policies, about	Individual Taxpayer Identification Numbers
implementation 293	(ITIN) 831
User Groups 292	International Traffic in Arms Regulations
policy conditions	(ITAR) 832
Content Matches data identifier 552	Media Files 833
policy detection	Merger and Acquisition Agreements 834
endpoint 632	NASD Rule 2711 and NYSE Rules 351 and
endpoint application 634	472 835
endpoint events 298	NASD Rule 3010 and NYSE Rule 342 837
endpoint protocol 632	NERC Security Guidelines for Electric
file contents 297	Utilities 838
file properties 297	Network Diagrams 839
identifiable file format types 669	Network Security 840
identities 298	Offensive Language 840
international languages 604	Office of Foreign Assets Control (OFAC) 841
introduction 296	OMB Memo 06-16 and FIPS 199
languages 298	Regulations 843
mobile 297	Password Files 844
network 297	Payment Card Industry (PCI) Data Security
rule severity 289	Standards 845
similarity score 528	PIPEDA 846
technologies 298	Price Information 848
using VML as an exception 533	Project Data 849
Vector Machine Learning (VML) 509	Proprietary Media Files 849
policy detection template, configuration	Publishing Documents 850
Yahoo Message Board 869	Racist Language 851
policy detection templates, configuration	Restricted Files 851
Caldicott Report 802	Restricted Recipients 851
CAN-SPAM Act 805	Resumes 852
Canadian Social Insurance Numbers 804	Sarbanes-Oxley 853
Common Spyware Upload Sites 806	SEC Fair Disclosure Regulation 855
Competitor Communications 806	Sexually Explicit Language 857
Credit Card Numbers 808	Source Code 858
Customer Data Protection 808	SWIFT Codes 862
Defense Message System (DMS) GENSER Classification 813	Symantec DLP Awareness and Avoidance 863 UK Data Protection Act 1998 810
Design Documents 814	UK Drivers License Numbers 863

policy detection templates, configuration <i>(continued)</i>	policy detection, keyword matching (continued)
UK Electoral Roll Numbers 864	wildcards, about support for 584
UK National Health Service (NHS) Number 864	policy detection, keyword matching, configuration
UK National Insurance Numbers 864	Content Matches Keyword 591
UK Passport Numbers 865	policy detection, keyword proximity
UK Tax ID Numbers 865	about 586
US Intelligence Control Markings (CAPCO) and	policy detection, regular expressions
DCID 1/7 866	Content Matches Regular Expression 600
US Social Security Numbers 867	implementing 598
Violence and Weapons 867	writing 598
Webmail 868	policy exceptions
policy detection,	add 337
endpoint destination 633	compound 342
policy detection, about	configure 340
keyword matching 584	policy exceptions, configure
policy detection, classification	match counting 334
Enabling test mode when 621	policy groups
policy detection, conditions	about 287
Content Matches Keyword 591	create 348
Content Matches Regular Expression 600	default policy group 287
Endpoint Device Class or ID 638	deployment 288
Endpoint Location 637	managing 347
Protocol or Endpoint Monitoring 635	modify 348
Recipient matches User Group based on a	removing 351
Directory Server Group 658	policy match condition
Sender/User Matches Pattern 645	Message/Email Properties and Attributes 623
Sender/User matches User Group based on a	policy match conditions
Directory Server Group 657	compound 308
policy detection, configuration	content 301
select message components to match on 336	content based on index 301
policy detection, described identities	cross-component matching 305
about 643	endpoint 304
Sender/User Matches Pattern 645	exceptions 307
policy detection, endpoint	file properties 302
devices, about 634	identities and groups 304
devices, add 639	message components 305
devices, adding 641	network and mobile 303
devices, configuring 641	server execution logic 308
devices, manage 639	simple 308
Endpoint Device Class or ID 638	subject matching 621
Endpoint Location 637	two-tier detection 309
locations, about 634	types 300
Protocol or Endpoint Monitoring 635	policy rules
policy detection, international	compound 342
data identifiers 606	policy rules, conditions
find keywords 606	configure 330
policy detection, keyword matching	policy rules, configuration
exmaples 587	rule severity 333
implementing 584	

1562

policy rules, configure	proxy servers 1165, 1542
match counting 334	compatibility with 1171, 1549
policy rules, detection	configuring 1170, 1172-1173, 1548-1550,
add 328	
policy rules, group	Q
add 328	guarantine files 1258
policy templates	quarantine nies 1256
add 325	_
Confidential Documents 807	R
create policy from 312	reflecting mode 1154–1155
Customer and Employee Data Protection 317	remediation 940
export 292, 350	commands 945
HIPAA and HITECH (including PHI) 826	email response variables 946
import 292, 349	Remote EDM Indexer utility
State Data Privacy 859	command-line options for 445
system-defined 286	creating EDM profile with 436
UK and International Regulatory	installation, Linux 449
Enforcement 317	installation, windows 448
US Regulatory Enforcement 315	installing 435
policy templates, configure	introducing 275
Exact Data Profile, select 322	requirements for using 434
Indexed Document Profile, select 323	running 434, 436, 442
policy templates, international	troubleshooting 447
about 605	uninstalling, Linux 449
policy templates, type	uninstalling, windows 448
Confidential or Classified Data Protection 319	Reporting API 1030
Network Security Enforcement 320	Reporting API privileges 95
Yahoo and MSN Messengers on Port 80 870	reports 961, 977, 986, 1006
policy templates, types	dashboards 1011
Acceptable Use Enforcement 320	incidents 1009
policy testing	list of options 1039
attachment 528	summaries 1016
test corpus 528	system events 135
policy violation headers 1163	REQMOD 1170, 1172, 1548-1549
enabling 1163	RequestProcdessor settings 1163
print/fax 1372	RequestProcessor fields 1158, 1161, 1164
processGets field 1174, 1551	RESPMOD 1170, 1172, 1548, 1562-1563
product suite. See Symantec Data Loss Prevention	response filtering 1169, 1545, 1561
profile tuning	response rules 954
how to 528	about 875
similarity threshold 528	add 889
properies	best practices 887
default similarity threshold 529	composing email responses 944
properties	configure 891
	manage 889
minimum number of documents per training set 529	modify ordering 895
	response rules, about
minimum number of features to keep 529 significance of features threshold 529	actions 875
Significance of realtires unleshold 329	authoring privileges 885

response rules, about (continued)	response rules, type
automated 881	Endpoint Prevent Block 1376
conditions 882	Endpoint Prevent Notify 1376
execution 880	Endpoint Prevent User Cancel 1377
execution priority for actions 883	Endpoint Quarantine 1388
implementation 886	response rules, types
removing 896	all detection servers 876
Smart 881	classification 880
Smart, configure 892	endpoint 877
response rules, actions	network 878
Add Note 906	network protect 879
Classify Enterprise Vault Content 915	restore
configure 893	archived incidents 1066
discarding network incident data 908	restricted ports 1158-1159
Endpoint Discover: Quarantine File 920	Retention categories 917
Endpoint Prevent Block 922	Revocation checks
Endpoint Prevent Notify, configuration 924	configuring 120
Endpoint Prevent User Cancel,	support for 118
configurations 928	roles
Endpoint: FlexResponse 919	add 103
Limit Incident Data Retention 906	adding 91
Log to a Syslog Server 909	configuring 91
Mobile Prevent Block FTP Request 931	manage 103
Mobile Prevent Block HTTP/S 931	roles, about
Network Prevent Block FTP Request 931	configuring 88
Network Prevent Block HTTP/S 931	recommended 88
Network Prevent: Block SMTP Message 933	role-based access control 84
Network Prevent: Modify SMTP Message 934	solution pack, included with 90
Network Prevent: Remove HTTP/HTTPS	RRC. See rules results caching
Content 935	rules results caching 1403
Network Protect Copy File 937	Tallog Foodillo Gadrining
Network Protect Quarantine File,	S
configuration 937	
retaining endpoint incident data 907	scans
Send Email Notification 910	differential scans 1222
Set Attribute 913	incremental scans 1222–1224
Set Status 914	Secure Computing Secure Web 1171
response rules, adding	Server Detail screen 201
Automated 890	server configuration 180
Smart 890	Server FlexResponse
response rules, conditions	configuring 912, 1232–1233
configure 892	configuring a response rule action with 912
endpoint device 898	configuring custom properties for 1233
endpoint location 897	deploying a plug-in for 1231–1233
incident match count 900	overview of 1228
incident thatch count 900	remediating with 1230, 1237–1238
protocol or endpoint monitoring 901	troubleshooting 1239
severity 903	Using a smart response action with 1237
Severity 303	servers (DLP). See detection servers and Enforce Server

ServerSocketPort field 1158	Symantec DLP Agent (continued)
Service_Shutdown.exe tool 1525	removing on Windows Vista 1499
Service_Shutdown.exe utility 276	removing with system management software
services 277	(SMS) 1498
SharePoint targets 1274	Symantec DLP services
Single-Tier Server 194	starting 80-82
sizing, profiles	stopping 80–83
memory allocation 537	Symantec Web Gateway 1171
significance threshold 537	syslog servers 144
sizing, training sets	system accounts 277
minimum 50 536	system alerts
recommended 250 536	about 146
SMTP 1161	adding 147
snapshots 961, 986	configuring server 146
SOAP messages 247	modifying 147
SPAN 1141, 1144	system events 134
SQL 276	code numbers 150
SQL Preindexer utility	event details 139
command-line options for 443	notification methods 135
introducing 275	reports 135
troubleshooting 446	reports, filtering 136
Squid Web Proxy 1171	reports, saved 138
SSL certificates	responses 142
importing 197	syslog servers 144
sslkeytool utility	thresholds, configuring 140
introducing 275	types (severities) of 140
status attributes 1069	System Overview screen 198
status groups	detection server, adding 194
adding 1072	errors and warning list 200
configuring 1072	server status 198
deleting 1072	system reports
status values	scheduling 1025
adding 1071	system setup, initial 58
configuring 1071	system upgrades 174
deleting 1071	
summary reports 961, 986	T
Switch Port Analyzer. See SPAN	
Symantec Data Loss Prevention	TagHighestSeverity field 1164
administration of 55	TagPolicyCount field 1164
initial system setup 58	TagScore field 1164
product suite 47	telnet command 1160
Symantec Data Loss Prevention servers. See	Test mode 621
detection servers and Enforce Server	TLS proxies 184, 1159
Symantec DLP Agent	Tomcat
administration 1457	adding certificates to 114
advanced settings 1414	changing trust store password for 115
agent store 1414	tools password 1518
removing 1497	training
removing manually 1500	cross-fold 538
- · · · · · · · · · · · · · · · · · · ·	k-fold evaluation process 538

training set	Vector Machine Learning (VML) (continued)
negative 535	adjusting memory allocation 520
positive 535	configuring VML exceptions 526
trial mode 184, 1155, 1168, 1544, 1561	configuring VML rules 525
troubleshooting	creating new VML profiles 515
debug log files 531	Currernt Profile tab 515
property configuration 529	editing profile name, description 524
training set quality 538	implementation process 513
	manage training sets 521
U	manage VML profiles 522
uninstalling 1520	rejecting training 511
upgrades, system 174	similarity score 512
user agents 1168, 1544	similarity threshold 512
User Groups	Temporary Workspace tab 515
creation 654	training content 510
user risk 1081	training the profile 518
user data sources 1083	uploading contents for training 516
adding 1084	violated policies 1163
adding from a file 1085	Vontu services
adding from Active Directory 1086	starting 77–82
defining custom attributes 1084	stopping 77–83
user details 1090	vontu_sqlite3.exe tool 1526
user list 1090	vontu_sqlite3.exe utility 276
user risk summary 1091	VPN
users	about 1538
add 104	14/
manage 104	W
users, about	Web archives 1073
configuring 88	Web Services 95
users, accounts	Websense V-Series 1172
adding 99	Webwasher 1171
configuring 99	WinPcap software 1145
users, authentication	installing 1146
Active Directory 105	
configuring Enforce for Active Directory	X
authentication 109	X-CFilter-Loop: Reflected header 1159
integrating Enforce with Active Directory 106	X-DLP-Max-Severity header 1164
verifying the Active Directory connection 108	X-DLP-Policy-Count header 1164
users, passwords	X-DLP-Score header 1164
configuring strong or rotating 102	XML schemas 1030
utilities	
introducing 274–275	
V	
-	
Vector Machine Learning (VML) about 509	
accepting training 511	
adjust similarity threshold 527	