

# Symantec™ Data Loss Prevention Administration Guide

Version 11.0



# Symantec Data Loss Prevention Administration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 11.0

## Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec 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 License Agreements* document 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 automatic software upgrades protection
- 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 web site at the following URL:

[www.symantec.com/business/support/](http://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/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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 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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

## Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

[www.symantec.com/business/services/](http://www.symantec.com/business/services/)

Select your country or language from the site index.

# Contents

Technical Support .....	4
Section 1    Getting started .....	33
Chapter 1    Introducing Symantec Data Loss Prevention .....	35
About Symantec Data Loss Prevention .....	35
About the Enforce platform .....	37
About Network Monitor and Prevent .....	38
About Network Discover .....	39
About Network Protect .....	40
About Endpoint Discover .....	40
About Endpoint Prevent .....	41
About Data Classification for Enterprise Vault .....	41
Chapter 2    Getting started administering Symantec Data Loss Prevention .....	45
About Symantec Data Loss Prevention administration .....	45
About the Enforce Server administration console .....	46
Logging on and off the Enforce Server administration console .....	47
About the administrator account .....	48
Performing initial setup tasks .....	48
Changing the administrator password .....	49
Adding an administrator email account .....	50
Editing a user profile .....	50
Changing your password .....	53
Chapter 3    Working with languages and locales .....	55
About support for character sets, languages, and locales .....	55
Supported languages for detection .....	56
Working with international characters .....	58
About Symantec Data Loss Prevention language packs .....	59
About locales .....	60
Using a non-English language on the Enforce Server administration console .....	61

	Using the Language Pack Utility .....	62
Section 2	Managing the Enforce Server platform .....	67
Chapter 4	Managing Enforce Server services and settings .....	69
	About Enforce Server services .....	69
	About starting and stopping services on Windows .....	70
	Starting an Enforce Server on Windows .....	70
	Stopping an Enforce Server on Windows .....	70
	Starting a Detection Server on Windows .....	71
	Stopping a Detection Server on Windows .....	71
	Starting services on single-tier Windows installations .....	72
	Stopping services on single-tier Windows installations .....	72
	Starting and stopping services on Linux .....	73
	Starting an Enforce Server on Linux .....	73
	Stopping an Enforce Server on Linux .....	74
	Starting a detection server on Linux .....	74
	Stopping a detection server on Linux .....	74
	Starting services on single-tier Linux installations .....	75
	Stopping services on single-tier Linux installations .....	75
Chapter 5	Managing roles and users .....	77
	About role-based access control .....	77
	About configuring roles and users .....	78
	About recommended roles for your organization .....	79
	Roles included with solution packs .....	80
	Configuring roles .....	82
	Configuring user accounts .....	89
	Configuring password enforcement settings .....	90
	Manage and add roles .....	91
	Manage and add users .....	92
	Integrating Active Directory for user authentication .....	92
	Creating the configuration file for Active Directory integration .....	93
	Verifying the Active Directory connection .....	95
	Configuring the Enforce Server for Active Directory authentication .....	96

Chapter 6	Managing stored credentials .....	99
	About the credential store .....	99
	Adding new credentials to the credential store .....	100
	Configuring endpoint credentials .....	100
	Managing credentials in the credential store .....	101
Chapter 7	Managing system events and messages .....	103
	About system events .....	103
	System events reports .....	104
	Working with saved system reports .....	107
	Server event detail .....	108
	Configuring event thresholds and triggers .....	109
	About system event responses .....	111
	Enabling a syslog server .....	113
	About system alerts .....	115
	Configuring the Enforce Server to send email alerts .....	115
	Configuring system alerts .....	117
	About log review .....	119
	System event codes and messages .....	119
Chapter 8	Adding a new product module .....	135
	Installing a new license file .....	135
	About system upgrades .....	136
Chapter 9	Migrating Symantec Data Loss Prevention servers to 64-bit operating systems .....	137
	Migrating Symantec Data Loss Prevention servers from 32-bit to 64-bit operating systems .....	137
	Migrating the Enforce Server to a 64-bit operating system .....	140
	Migrating a detection server to a 64-bit operating system .....	143
Section 3	Managing detection servers .....	147
Chapter 10	Installing and managing detection servers .....	149
	About managing Symantec Data Loss Prevention servers .....	150
	Enabling Advanced Process Control .....	150
	Server controls .....	151
	Server configuration—basic .....	152
	Network Monitor Server—basic configuration .....	154

	Network Prevent (Email) Server—basic configuration .....	156
	Network Prevent (Web) Server—basic configuration .....	159
	Network Discover Server and Network Protect—basic configuration .....	162
	Endpoint Server—basic configuration .....	163
	Classification Server—basic configuration .....	164
	Server configuration—advanced .....	165
	Adding a detection server .....	166
	Removing a server .....	167
	Importing SSL certificates to Enforce or Discover servers .....	168
	About the System Overview screen .....	169
	Server status overview .....	170
	Recent error and warning events list .....	172
	Server Detail screen .....	172
	Advanced server settings .....	174
	Advanced agent settings .....	204
<b>Chapter 11</b>	<b>Managing log files .....</b>	<b>225</b>
	About log files .....	225
	Operational log files .....	226
	Debug log files .....	228
	Log collection and configuration screen .....	231
	Configuring server logging behavior .....	231
	Collecting server logs and configuration files .....	236
	About log event codes .....	241
	Network Prevent (Web) operational log files and event codes .....	241
	Network Prevent (Web) access log files and fields .....	243
	Network Prevent (Web) protocol debug log files .....	244
	Network Prevent (Email) log levels .....	245
	Network Prevent (Email) operational log codes .....	246
	Network Prevent (Email) originated responses and codes .....	249
<b>Chapter 12</b>	<b>Using Symantec Data Loss Prevention utilities .....</b>	<b>253</b>
	About the Symantec Data Loss Prevention utilities .....	253
	About Endpoint utilities .....	255
	About the Environment Check Utility .....	256
	Running the Environment Check Utility on Windows .....	257
	Running the Environment Check Utility on Linux .....	257
	About Environment Check Utility output .....	258
	About DBPasswordChanger .....	258
	DBPasswordChanger syntax .....	259

Example of using DBPasswordChanger .....	259
About the sslkeytool utility and server certificates .....	260
About sslkeytool command line options .....	261
Using sslkeytool to generate new Enforce and detection server certificates .....	262
Using sslkeytool to add new detection server certificates .....	264
Verifying server certificate usage .....	265
About the SQL Preindexer .....	265
SQL Preindexer command function and options .....	266
Troubleshooting preindexing errors .....	267
About the Remote EDM Indexer .....	268
System requirements for the Remote EDM Indexer .....	268
Using the Remote EDM Indexer .....	269
Installing the Remote EDM Indexer .....	269
Installing from the command line (for Linux) .....	270
Creating an EDM profile for remote indexing .....	271
Remote EDM Indexer command options .....	274
Copying and using generated index files .....	275
Troubleshooting index jobs .....	276
Uninstalling Remote Indexer on a Windows platform .....	277
Uninstalling Remote Indexer on a Linux platform .....	277
 Section 4	
Implementing policy detection .....	279
 Chapter 13	
Detecting data loss .....	281
Introduction to policy detection .....	281
About content that can be detected .....	281
About file types that can be detected .....	282
About network incidents that can be detected .....	282
About endpoint events that can be detected .....	282
About identities that can be detected .....	283
About languages that can be detected .....	283
Available detection technologies .....	283
About Exact Data Matching .....	284
About Indexed Document Matching .....	285
About Described Content Matching .....	286
About Directory Group Matching .....	287
About custom detection .....	287
Introduction to detection rules .....	288
Content matching conditions .....	289
File property matching conditions .....	290
Network protocol matching condition .....	291

	Endpoint matching conditions .....	291
	Groups (identities) matching conditions .....	292
	About message components that can be matched .....	293
	About rule severity .....	295
	About rule exceptions .....	296
	About compound match conditions .....	297
	About detection execution .....	297
	Implementing policy detection .....	299
	About developing a data loss prevention strategy .....	300
	About policy detection development .....	301
	About achieving precise detection results .....	301
	About common detection problems to avoid .....	302
	About using the appropriate detection method .....	303
	About using exceptions to narrow detection scope .....	304
	About using compound rules for precise detection .....	305
Chapter 14	Policy authoring .....	307
	About policies .....	307
	About policy components .....	309
	About system-defined policy templates .....	310
	About solution packs .....	311
	About policy groups .....	311
	About policy deployment .....	312
	About policy authoring privileges .....	313
	About policy template import and export .....	314
	About Data Profiles .....	316
	About User Groups .....	317
	Implementing policies .....	317
	Policy best practices .....	318
Chapter 15	Creating policies from templates .....	321
	Creating a policy from a template .....	321
	US Regulatory Enforcement policy templates .....	324
	UK and International Regulatory Enforcement policy templates .....	327
	Customer and Employee Data Protection policy templates .....	327
	Confidential or Classified Data Protection policy templates .....	329
	Network Security Enforcement policy templates .....	330
	Acceptable Use Enforcement policy templates .....	331
	Choosing an Exact Data Profile .....	333
	Choosing an Indexed Document Profile .....	334

Chapter 16	Configuring policies .....	337
	Adding a new policy or policy template .....	337
	Configuring policies .....	338
	Adding a rule to a policy .....	340
	Configuring policy rules .....	342
	Defining rule severity .....	345
	Configuring match counting .....	346
	Selecting components to match on .....	348
	Adding an exception to a policy .....	349
	Configuring policy exceptions .....	351
	Configuring compound match conditions .....	354
Chapter 17	Administering policies .....	357
	Manage and add policies .....	357
	Creating and modifying policy groups .....	359
	Manage and add policy groups .....	360
	Importing policy templates .....	361
	Exporting policy detection as a template .....	362
	Importing version 10 data identifier or keyword policies to version 11 systems .....	362
	Adding a response rule to a policy .....	363
	About removing policies and policy groups .....	364
Chapter 18	Detecting content using Exact Data Matching .....	367
	About implementing Exact Data Matching .....	368
	Implementing Exact Data Matching .....	368
	About data owner exception .....	370
	About field mappings .....	370
	About index scheduling .....	371
	About configuring exact data match counting .....	371
	Manage and add Exact Data Profiles .....	372
	Creating the exact data source file .....	374
	Migrating legacy data owner exception configurations .....	375
	Preparing the exact data source file for indexing .....	376
	Uploading exact data source files to the Enforce Server .....	378
	Creating and modifying Exact Data Profiles .....	379
	Mapping Exact Data Profile fields .....	384
	Scheduling Exact Data Profile indexing .....	386
	Configuring the Content Matches Exact Data condition .....	387
	EDM best practices .....	390

Chapter 19	Detecting content using Index Document Matching .....	393
	About implementing Indexed Document Matching .....	393
	Detectable content types .....	395
	Manage and add Indexed Document Profiles .....	400
	Implementing Indexed Document Matching .....	402
	Preparing the document source for indexing .....	403
	Excluding (whitelisting) content from detection .....	404
	Creating and modifying Indexed Document Profiles .....	405
	Filtering documents by file name and size .....	408
	Scheduling document profile indexing .....	409
	Configuring the Content Matches Document Signature condition .....	411
	IDM best practices .....	412
Chapter 20	Detecting content using data identifiers .....	415
	About data identifiers .....	416
	Available system data identifiers .....	417
	About data identifier breadths .....	420
	About optional validators .....	421
	Acceptable characters for optional validators .....	422
	About cross-component matching for data identifiers .....	425
	About modifying data identifiers .....	425
	About data identifier patterns .....	426
	About validators .....	426
	About custom data identifiers .....	429
	About data normalizers .....	430
	About data identifier configuration .....	430
	Manage and add data identifiers .....	433
	Configuring the Content Matches Data Identifier condition .....	434
	Selecting system data identifier breadth .....	436
	Configuring optional validators .....	440
	Modifying and creating data identifiers .....	441
	Manually cloning a system data identifier before modifying it .....	442
	Editing required validator input .....	442
	Implementing custom data identifiers .....	443
	Implementing patterns to match data .....	444
	Selecting required data validators .....	445
	Implementing custom script validators .....	446
	Data identifier best practices .....	447

Chapter 21	Detecting content using keyword matching .....	449
	About implementing keyword matching .....	449
	About keyword proximity matching .....	450
	Keyword matching examples .....	451
	Configuring the Content Matches Keyword condition .....	452
	About profiling keyword dictionaries .....	455
	Keyword matching best practices .....	456
Chapter 22	Detecting content using regular expressions .....	457
	About regular expression matching .....	457
	Configuring the Content Matches Regular Expression condition .....	457
	About writing regular expressions .....	459
	Regular expression detection best practices .....	460
Chapter 23	Detecting file properties .....	463
	About implementing file property matching .....	463
	About file type detection .....	464
	Detectable file types .....	465
	About custom file type detection .....	479
	About file size detection .....	480
	About file name detection .....	480
	File name detection examples .....	481
	Configuring the Message Attachment or File Type Match condition .....	481
	Configuring the Message Attachment or File Size Match condition .....	482
	Configuring the Message Attachment or File Name Match condition .....	483
	Enabling custom file type detection .....	484
	Configuring the Custom File Type Signature condition .....	485
	File property detection best practices .....	486
Chapter 24	Detecting network incidents .....	487
	About network protocol matching .....	487
	Configuring Protocol Monitoring condition parameters .....	488
Chapter 25	Detecting endpoint events .....	491
	About implementing endpoint event detection .....	491
	About endpoint protocol, destination, and application detection .....	492
	About endpoint device detection .....	492

	About endpoint location detection .....	493
	Configuring Endpoint Monitoring condition parameters .....	493
	Gathering endpoint device IDs .....	496
	Manage and add endpoint devices .....	496
	Creating and modifying endpoint device configurations .....	497
	Configuring the Endpoint Device Class or ID condition .....	498
	Configuring the Endpoint Location condition .....	499
	Endpoint detection best practices .....	500
Chapter 26	Detecting described identities .....	503
	About described identity matching .....	503
	Configuring the Sender/User Matches Pattern condition .....	504
	Configuring the Recipient Matches Pattern condition .....	506
	Described identity matching best practices .....	508
Chapter 27	Detecting synchronized identities .....	511
	About implementing synchronized Directory Group Matching .....	511
	About connecting to directory group servers .....	513
	Creating and managing directory server connections .....	513
	Scheduling directory server indexing .....	516
	Creating or modifying a User Group .....	517
	Configuring the Sender/User matches User Group based on a Directory Server condition .....	519
	Configuring the Recipient Matches User Group based on a Directory Server condition .....	520
	Synchronized DGM best practices .....	521
Chapter 28	Detecting profiled identities .....	523
	About implementing profiled Directory Group Matching .....	523
	Creating the Exact Data Profile for static DGM .....	524
	Configuring the Sender/User Matches Directory From Exact Data Profile condition .....	525
	Configuring the Recipient Matches Directory From Exact Data Profile condition .....	526
	Profiled DGM best practices .....	527
Chapter 29	Detecting international content .....	529
	About implementing non-English language detection .....	529
	International policy templates .....	530
	Using find keywords for international system data identifiers .....	531
	Detecting non-English document content .....	533

Chapter 30	System data identifiers .....	535
	ABA Routing Number system data identifier .....	536
	ABA Routing Number wide breadth .....	537
	ABA Routing Number medium breadth .....	537
	ABA Routing Number narrow breadth .....	538
	Australian Medicare Number system data identifier .....	539
	Australian Tax File Number system data identifier .....	540
	Burgerservicenummer system data identifier .....	540
	Canadian Social Insurance Number system data identifier .....	541
	Canadian Social Insurance Number wide breadth .....	541
	Canadian Social Insurance Number medium breadth .....	542
	Canadian Social Insurance Number narrow breadth .....	542
	Codice Fiscale system data identifier .....	543
	Credit Card Magnetic Stripe Data system data identifier .....	544
	Credit Card Number system data identifier .....	546
	Credit Card Number wide breadth .....	546
	Credit Card Number medium breadth .....	547
	Credit Card Number narrow breadth .....	549
	CUSIP Number system data identifier .....	552
	CUSIP Number wide breadth .....	552
	CUSIP Number medium breadth .....	553
	CUSIP Number narrow breadth .....	553
	Drivers License Number – CA State system data identifier .....	554
	Drivers License Number – CA State wide breadth .....	554
	Drivers License Number – CA State medium breadth .....	555
	Drivers License Number - FL, MI, MN States system data identifier .....	556
	Drivers License Number- FL, MI, MN States wide breadth .....	556
	Drivers License Number- FL, MI, MN States medium breadth .....	556
	Drivers License Number - IL State system data identifier .....	557
	Drivers License Number- IL State wide breadth .....	558
	Drivers License Number- IL State medium breadth .....	558
	Drivers License Number - NJ State system data identifier .....	559
	Drivers License Number- NJ State wide breadth .....	559
	Drivers License Number- NJ State medium breadth .....	560
	Drivers License Number - NY State system data identifier .....	560
	Drivers License Number- NY State wide breadth .....	561
	Drivers License Number - NY State medium breadth .....	561
	French INSEE Code system data identifier .....	562
	Hong Kong ID system data identifier .....	562
	IBAN Central system data identifier .....	563

IBAN East system data identifier .....	565
IBAN West system data identifier .....	568
IP Address system data identifier .....	570
IP Address wide breadth .....	570
IP Address medium breadth .....	571
IP Address narrow breadth .....	572
National Drug Code (NDC) system data identifier .....	572
National Drug Code (NDC) wide breadth .....	573
National Drug Code (NDC) medium breadth .....	573
National Drug Code (NDC) narrow breadth .....	574
People's Republic of China ID system data identifier .....	575
Singapore NRIC system data identifier .....	575
South Korea Resident Registration Number system data identifier .....	576
South Korea Resident Registration Number wide breadth .....	576
South Korea Resident Registration Number medium breadth .....	577
Spanish DNI ID system data identifier .....	577
SWIFT Code system data identifier .....	578
SWIFT Code wide breadth .....	578
SWIFT Code narrow breadth .....	579
Swiss AHV Number system data identifier .....	580
Taiwan ROC ID system data identifier .....	580
UK Drivers License Number system data identifier .....	581
UK Drivers License Number wide breadth .....	581
UK Drivers License Number medium breadth .....	582
UK Drivers License Number narrow breadth .....	582
UK Electoral Roll Number system data identifier .....	583
UK National Health Service (NHS) Number system data identifier .....	584
UK National Health Service (NHS) Number medium breadth .....	585
UK National Health Service (NHS) Number narrow breadth .....	585
UK National Insurance Number system data identifier .....	586
UK National Insurance Number wide breadth .....	587
UK National Insurance Number medium breadth .....	587
UK National Insurance Number narrow breadth .....	588
UK Passport Number system data identifier .....	589
UK Passport Number wide breadth .....	589
UK Passport Number medium breadth .....	589
UK Passport Number narrow breadth .....	590
UK Tax ID Number system data identifier .....	591
UK Tax ID Number wide breadth .....	591

UK Tax ID Number medium breadth ..... 592

UK Tax ID Number narrow breadth ..... 592

US Individual Tax Identification Number (ITIN) system data  
 identifier ..... 593

US Individual Tax Identification Number (ITIN) wide  
 breadth ..... 594

US Individual Tax Identification Number (ITIN) medium  
 breadth ..... 594

US Individual Tax Identification Number (ITIN) narrow  
 breadth ..... 595

US Social Security Number (SSN) system data identifier ..... 596

US Social Security Number (SSN) wide breadth ..... 596

US Social Security Number (SSN) medium breadth ..... 598

US Social Security Number (SSN) narrow breadth ..... 599

Chapter 31 Policy templates ..... 601

Caldicott Report policy template ..... 603

Canadian Social Insurance Numbers policy template ..... 605

CAN-SPAM Act policy template ..... 605

Common Spyware Upload Sites policy template ..... 607

Competitor Communications policy template ..... 607

Confidential Documents policy template ..... 608

Credit Card Numbers policy template ..... 609

Customer Data Protection policy template ..... 609

Data Protection Act 1998 (UK) policy template ..... 611

Data Protection Directives (EU) policy template ..... 612

Defense Message System (DMS) GENSER Classification policy  
 template ..... 613

Design Documents policy template ..... 615

Employee Data Protection policy template ..... 616

Encrypted Data policy template ..... 617

Export Administration Regulations (EAR) policy template ..... 618

FACTA 2003 (Red Flag Rules) policy template ..... 619

Financial Information policy template ..... 623

Forbidden Websites policy template ..... 624

Gambling policy template ..... 624

Gramm-Leach-Bliley policy template ..... 625

HIPAA and HITECH (including PHI) policy template ..... 627

Human Rights Act 1998 policy template ..... 631

Illegal Drugs policy template ..... 632

Individual Taxpayer Identification Numbers (ITIN) policy  
 template ..... 633

International Traffic in Arms Regulations (ITAR) policy	
template .....	633
Media Files policy template .....	634
Merger and Acquisition Agreements policy template .....	635
NASD Rule 2711 and NYSE Rules 351 and 472 policy template .....	637
NASD Rule 3010 and NYSE Rule 342 policy template .....	638
NERC Security Guidelines for Electric Utilities policy template .....	640
Network Diagrams policy template .....	642
Network Security policy template .....	643
Offensive Language policy template .....	643
Office of Foreign Assets Control (OFAC) policy template .....	644
OMB Memo 06-16 and FIPS 199 Regulations policy template .....	646
Password Files policy template .....	647
Payment Card Industry (PCI) Data Security Standard policy	
template .....	648
PIPEDA policy template .....	649
Price Information policy template .....	651
Project Data policy template .....	652
Proprietary Media Files policy template .....	652
Publishing Documents policy template .....	653
Racist Language policy template .....	654
Restricted Files policy template .....	654
Restricted Recipients policy template .....	655
Resumes policy template .....	655
Sarbanes-Oxley policy template .....	656
SEC Fair Disclosure Regulation policy template .....	658
Sexually Explicit Language policy template .....	660
Source Code policy template .....	661
State Data Privacy policy template .....	662
SWIFT Codes policy template .....	666
Symantec DLP Awareness and Avoidance policy template .....	666
UK Drivers License Numbers policy template .....	667
UK Electoral Roll Numbers policy template .....	667
UK National Health Service (NHS) Number policy template .....	668
UK National Insurance Numbers policy template .....	668
UK Passport Numbers policy template .....	669
UK Tax ID Numbers policy template .....	669
US Intelligence Control Markings (CAPCO) and DCID 1/7 policy	
template .....	669
US Social Security Numbers policy template .....	671
Violence and Weapons policy template .....	671
Webmail policy template .....	671
Yahoo Message Board Activity policy template .....	672

	Yahoo and MSN Messengers on Port 80 policy template .....	674
Section 5	Configuring policy response .....	677
Chapter 32	Responding to policy violations .....	679
	About response rules .....	680
	About response rule actions .....	680
	Response rules for all detection servers .....	681
	Response rules for Endpoint detection .....	682
	Response rules for Network detection .....	683
	Response rule for the Classification Server .....	684
	About response rule execution types .....	685
	About Automated response rules .....	686
	About Smart response rules .....	686
	About response rule conditions .....	687
	About response rule action execution priority .....	688
	About response rule authoring privileges .....	690
	Implementing policy response rules .....	691
	Response rule best practices .....	692
Chapter 33	Configuring and managing response rules .....	695
	Manage response rules .....	695
	Adding a new response rule .....	697
	Configuring response rules .....	697
	About configuring Smart response rules .....	698
	Configuring response rule conditions .....	698
	Configuring response rule actions .....	699
	Modifying response rule ordering .....	701
	About removing response rules .....	702
Chapter 34	Response rule conditions .....	703
	Configuring the Endpoint Location response condition .....	703
	Configuring the Endpoint Device response condition .....	704
	Configuring the Incident Type response condition .....	705
	Configuring the Incident Match Count response condition .....	707
	Configuring the Protocol or Endpoint Monitoring response condition .....	708
	Configuring the Severity response condition .....	711

Chapter 35	Response rule actions .....	713
	Configuring the Add Note action .....	714
	Configuring the Limit Incident Data Retention action .....	714
	Retaining data for endpoint incidents .....	715
	Discarding data for network incidents .....	716
	Configuring the Log to a Syslog Server action .....	717
	Configuring the Send Email Notification action .....	718
	Configuring the Set Attribute action .....	720
	Configuring the Set Status action .....	721
	Configuring the Endpoint: FlexResponse action .....	721
	Configuring the Endpoint Discover: Quarantine File action .....	722
	Configuring the Endpoint Prevent: Block action .....	725
	Configuring the Endpoint Prevent: Notify action .....	728
	Configuring the Endpoint Prevent: User Cancel action .....	731
	Configuring the Network Prevent: Block FTP Request action .....	734
	Configuring the Network Prevent: Block HTTP/S action .....	734
	Configuring the Network Prevent: Block SMTP Message action .....	736
	Configuring the Network Prevent: Modify SMTP Message action .....	737
	Configuring the Network Prevent: Remove HTTP/S Content action .....	738
	Configuring the Network Protect: Copy File action .....	740
	Configuring the Network Protect: Quarantine File action .....	740
Section 6	Managing data loss incidents .....	743
Chapter 36	Managing incident reports .....	745
	About Symantec Data Loss Prevention reports .....	745
	About strategies for using reports .....	747
	Setting report preferences .....	747
	About dashboard reports and executive summaries .....	748
	Viewing dashboards .....	749
	Creating dashboard reports .....	750
	About summary reports .....	751
	Viewing summary reports .....	752
	Creating summary reports .....	752
	About custom reports and dashboards .....	753
	Filtering reports .....	755
	Saving custom incident reports .....	755
	Scheduling custom incident reports .....	756
	Editing custom dashboards and reports .....	758
	Deleting custom dashboards and reports .....	759

Chapter 37	Report filters and summary options .....	761
	About filters and summary options for reports .....	761
	General filters for reports .....	763
	Advanced filter options for reports .....	766
	Summary options for reports .....	777
Chapter 38	About incident remediation .....	783
	About incident remediation .....	783
	Viewing incidents .....	786
	Remediating incidents .....	787
	Creating and distributing aggregated incident reports to data owners .....	788
Chapter 39	Managing custom attributes and status values for incidents .....	793
	About incident status attributes .....	793
	Configuring status attributes and values .....	795
	Configuring status groups .....	796
	About custom attributes .....	797
	Setting the values of custom attributes .....	799
	Configuring custom attributes .....	799
Section 7	Monitoring and preventing data loss in the network .....	801
Chapter 40	Implementing Network Monitor .....	803
	Implementing Network Monitor .....	803
	Choosing a network packet capture method .....	805
	About packet capture software installation and configuration .....	806
	Installing WinPcap on a Windows platform .....	806
	Updating the Endace card driver .....	807
	Configuring the Network Monitor Server .....	807
	Enabling GET processing with Network Monitor .....	809
	Creating a policy for Network Monitor .....	810
	Testing Network Monitor .....	810
Chapter 41	Implementing Network Prevent (Email) .....	813
	Implementing Network Prevent (Email) .....	813
	About Mail Transfer Agent (MTA) integration .....	815

	Configuring Network Prevent (Email) Server for reflecting or forwarding mode .....	816
	Configuring Linux IP tables to reroute traffic from a restricted port .....	820
	Specifying one or more upstream mail transfer agents (MTAs) .....	821
	Creating a policy for Network Prevent (Email) .....	822
	About policy violation data headers .....	824
	Enabling policy violation data headers .....	824
	Testing Network Prevent (Email) .....	825
Chapter 42	Implementing Network Prevent (Web) .....	827
	Implementing Network Prevent (Web) .....	827
	Configuring Network Prevent (Web) Server .....	829
	About proxy server configuration .....	832
	Proxy server compatibility with Network Prevent (Web) .....	833
	Configuring request and response mode services .....	833
	Specifying one or more proxy servers .....	835
	Enabling GET processing for Network Prevent (Web) .....	835
	Creating policies for Network Prevent (Web) .....	836
	Testing Network Prevent (Web) .....	838
	Troubleshooting information for Network Prevent (Web) Server .....	838
Section 8	Discovering where confidential data is stored .....	841
Chapter 43	About Network Discover .....	843
	About Network Discover .....	843
	How Network Discover works .....	845
Chapter 44	Setting up and configuring Network Discover .....	847
	Setting up and configuring Network Discover .....	847
	Modifying the Network Discover Server configuration .....	848
	About Linux Network Discover Servers .....	850
	Adding a new Network Discover target .....	850
	Editing an existing Network Discover target .....	852

Chapter 45	Network Discover scan target configuration options .....	855
	Network Discover scan target configuration options .....	855
	Configuring the required fields for Network Discover targets .....	857
	Scheduling Network Discover scans .....	858
	Providing the password authentication for Network Discover scanned content .....	860
	Encrypting passwords in configuration files .....	861
	Setting up Discover filters to include or exclude items from the scan .....	861
	Filtering Discover targets by item size .....	864
	Filtering Discover targets by date last accessed or modified .....	865
	Optimizing resources with Network Discover scan throttling .....	868
	Creating an inventory of the locations of unprotected sensitive data .....	869
Chapter 46	Managing Network Discover target scans .....	873
	Managing Network Discover target scans .....	874
	Network Discover scan target list .....	874
	Network Discover target scan status .....	875
	Network Discover scan detail .....	876
	Network Discover scan history .....	879
	About Network Discover scan optimization .....	880
	About the difference between incremental scans and differential scans .....	882
	About incremental scans .....	883
	Scanning new or modified files (an incremental scan) .....	884
	Managing incremental scans .....	885
	Scanning new or modified items (a differential scan) .....	886
	Configuring parallel scanning of Network Discover targets .....	886
	Removing Network Discover scan targets .....	887
	Deleting Network Discover scans .....	888
Chapter 47	Managing Network Discover incident reports .....	889
	About reports for Network Discover .....	889
	About incident reports for Network Discover .....	890

Chapter 48	Using FlexResponse custom plug-ins to remediate incidents .....	893
	Using Server FlexResponse custom plug-ins to remediate incidents .....	893
	Creating Response Rules that use incident response actions .....	894
	Locating incidents for remediation .....	895
	Using the action of a Server FlexResponse plug-in to remediate an incident .....	896
	Verifying the results of a manual incident response action .....	897
Chapter 49	Setting up scans of file shares .....	899
	Setting up scans of file shares .....	899
	Supported file share targets .....	900
	Excluding internal DFS folders .....	901
	Configuring scans of Microsoft Outlook Personal Folders (.pst files) .....	901
	Configuring and running scans of file shares .....	902
	Configuring Network Protect for file shares .....	906
Chapter 50	Setting up scans of Lotus Notes databases .....	909
	Setting up scans of Lotus Notes databases .....	909
	Supported Lotus Notes targets .....	910
	Configuring and running Lotus Notes scans .....	911
	Configuring Lotus Notes native mode configuration scan options .....	913
	Configuring Lotus Notes DIIOP mode configuration scan options .....	916
Chapter 51	Setting up scans of SQL databases .....	919
	Setting up scans of SQL databases .....	919
	Supported SQL database targets .....	920
	Configuring and running SQL database scans .....	920
	Installing the JDBC driver for SQL database targets .....	923
	SQL database scan configuration properties .....	924
Chapter 52	Setting up scans of SharePoint servers .....	927
	Setting up scans of SharePoint servers .....	927
	About scans of SharePoint servers .....	928
	Supported SharePoint server targets .....	930
	Access privileges for SharePoint 2007 and 2010 scans .....	930

	Configuring and running SharePoint server scans .....	931
	Installing the SharePoint solution on the Web Front Ends in a Farm .....	934
	Setting up SharePoint scans to use Kerberos authentication .....	936
	Troubleshooting SharePoint scans .....	937
Chapter 53	Setting up scans of Exchange servers .....	939
	Setting up scans of Exchange repositories .....	939
	About scans of Exchange servers .....	940
	Supported Exchange server targets .....	941
	Providing access rights to scan all mailboxes and public folders .....	942
	Configuring and running Exchange server scans .....	943
	Example configurations and use cases .....	947
	Troubleshooting Exchange scans .....	949
Chapter 54	About Network Discover scanners .....	951
	How Network Discover scanners work .....	951
	Troubleshooting scanners .....	952
	Scanner processes .....	955
	Scanner installation directory structure .....	955
	Scanner configuration files .....	957
	Scanner controller configuration options .....	958
Chapter 55	Setting up scanning of file systems .....	961
	Setting up scanning of file systems .....	962
	Supported file system (scanner) targets .....	963
	Installing file system scanners .....	964
	Starting file system scans .....	966
	Installing file system scanners silently from the command line .....	967
	Configuration options for file system scanners .....	968
	Example configuration for scanning the C drive on a Windows computer .....	969
	Example configuration for scanning the /usr directory on UNIX .....	970
	Example configuration for scanning with include filters .....	970
	Example configuration for scanning with exclude filters .....	971
	Example configuration for scanning with include and exclude filters .....	971
	Example configuration for scanning with date filtering .....	972
	Example configuration for scanning with file size filtering .....	972
	Example configuration for scanning that skips symbolic links on UNIX systems .....	973

Chapter 56	Setting up scanning of Microsoft Exchange servers .....	975
	Setting up scanning of Microsoft Exchange Servers .....	975
	Supported Exchange scanner targets .....	977
	Checking Exchange Mailbox Store permissions .....	978
	Installing Exchange scanners .....	979
	Configuration options for Exchange scanners .....	981
	Configuring the profile name .....	984
	Configuring settings for DNMailbox .....	985
	Starting Microsoft Exchange scans .....	985
	Example configuration for scanning the Exchange Archive Public Folder .....	987
	Example configuration for scanning an Exchange Inbox .....	987
	Example configuration for scanning another user's Inbox .....	988
	Example configuration for scanning all Exchange mailboxes .....	988
Chapter 57	Setting up scanning of SharePoint 2007 servers .....	991
	Setting up scanning of SharePoint 2007 servers .....	991
	Supported SharePoint scanner targets .....	993
	Access privileges for a SharePoint 2007 scan .....	994
	Installing SharePoint 2007 scanners .....	994
	Starting SharePoint 2007 scans .....	996
	Configuration options for SharePoint 2007 scanners .....	998
	Example configuration for scanning a specific site collection .....	1000
	Example configuration for scanning a specific Web site .....	1000
	Example configuration for scanning all Web sites from a Web application .....	1000
	Example configuration for scanning all Web sites from all Web applications present on the server .....	1000
	Scheduling SharePoint 2007 scanning .....	1001
Chapter 58	Setting up scanning of SharePoint 2003 servers .....	1003
	Setting up scanning of SharePoint 2003 servers .....	1003
	Installing SharePoint 2003 scanners .....	1004
	Starting SharePoint 2003 scans .....	1006
	Configuration options for SharePoint 2003 scanners .....	1008
	Example configuration for scanning all SharePoint 2003 sites .....	1009
	Example configuration for scanning one SharePoint 2003 site .....	1010

Chapter 59	Setting up scanning of Web servers .....	1011
	Setting up scanning of Web servers .....	1011
	Supported Web server (scanner) targets .....	1013
	Installing Web server scanners .....	1013
	Starting Web server scans .....	1015
	Configuration options for Web server scanners .....	1016
	Example configuration for a Web site scan with no authentication .....	1019
	Example configuration for a Web site scan with basic authentication .....	1019
	Example configuration for a Web site scan with form-based authentication .....	1020
	Example configuration for a Web site scan with NTLM .....	1020
	Example of URL filtering for a Web site scan .....	1021
	Example of date filtering for a Web site scan .....	1022
Chapter 60	Setting up scanning of Documentum repositories .....	1023
	Setting up scanning of Documentum repositories .....	1023
	Supported Documentum (scanner) targets .....	1024
	Installing Documentum scanners .....	1024
	Starting Documentum scans .....	1027
	Configuration options for Documentum scanners .....	1028
	Example configuration for scanning all documents in a Documentum repository .....	1030
Chapter 61	Setting up scanning of Livelink repositories .....	1033
	Setting up scanning of Livelink repositories .....	1033
	Supported Livelink (scanner) targets .....	1034
	Creating an ODBC data source for SQL Server .....	1034
	Installing Livelink scanners .....	1035
	Starting Livelink scans .....	1037
	Configuration options for Livelink scanners .....	1039
	Example configuration for scanning a Livelink database .....	1040
Chapter 62	Setting up Web Services for custom scan targets .....	1041
	Setting up Web Services for custom scan targets .....	1041
	About setting up the Web Services Definition Language (WSDL) .....	1042
	Example of a Web Services Java client .....	1042

	Sample Java code for the Web Services example .....	1043
Section 9	Discovering and preventing data loss on endpoint computers .....	1047
Chapter 63	Using Endpoint Discover and Endpoint Prevent .....	1049
	About Endpoint Discover and Endpoint Prevent .....	1049
	How Endpoint Discover works .....	1050
	How Endpoint Prevent works .....	1051
	About the Endpoint Server .....	1051
	About the Symantec DLP Agent .....	1052
	About Endpoint Prevent monitoring .....	1052
	About removable media monitoring .....	1053
	About CD/DVD monitoring .....	1054
	About print/fax monitoring .....	1055
	About clipboard monitoring .....	1056
	About application monitoring .....	1056
	About network share monitoring .....	1057
	About Endpoint network monitoring .....	1057
	About Endpoint Discover monitoring .....	1059
	About targeted Endpoint Discover scans .....	1060
	About policies for endpoint computers .....	1060
	About policy creation for Endpoint Prevent .....	1062
	About monitoring policies with response rules for Endpoint Servers .....	1062
	About rules results caching (RRC) .....	1065
	About Endpoint reports .....	1066
Chapter 64	Implementing Endpoint Discover .....	1067
	How to implement Endpoint Discover .....	1067
	Creating a policy group for Endpoint Discover .....	1068
	Creating a policy for Endpoint Discover .....	1068
	Adding a rule for Endpoint Discover .....	1069
	Setting up scanning of an Endpoint Discover target .....	1071
	Configuration options for endpoint targets .....	1072
Chapter 65	Implementing Endpoint Prevent .....	1075
	How to implement Endpoint Prevent .....	1075
	Setting the endpoint location .....	1076
	About Endpoint Prevent response rules in different locales .....	1077

Chapter 66	Working with agent configurations .....	1081
	About agent configurations .....	1081
	About cloning agent configurations .....	1082
	Adding agent configurations .....	1082
	Applying agent configurations to an Endpoint Server .....	1087
Chapter 67	Working with Endpoint FlexResponse .....	1089
	About Endpoint FlexResponse .....	1089
	Deploying Endpoint FlexResponse .....	1090
	Deploying Endpoint FlexResponse plug-ins on endpoint computers .....	1091
	Installing Endpoint FlexResponse plug-ins using a silent installation process .....	1092
	About the Endpoint FlexResponse utility .....	1092
	Loading Endpoint FlexResponse plug-ins using the Endpoint FlexResponse utility .....	1093
	Enabling Endpoint FlexResponse on the Enforce Server .....	1094
	Uninstalling Endpoint FlexResponse plug-ins using the FlexResponse utility .....	1095
	Retrieving Endpoint FlexResponse plug-ins from a specific endpoint computer .....	1095
	Retrieving a list of Endpoint FlexResponse plug-ins from an endpoint computer .....	1096
Chapter 68	Implementing Symantec DLP Agents .....	1097
	About the Symantec Management Console .....	1097
	Cloning advertisements and programs .....	1098
	Using computer discovery .....	1098
	Installing the Symantec Management Agent .....	1099
	About Symantec Management Console reporting .....	1100
	About Symantec Management Console agent tasks .....	1101
	Creating user tasks .....	1102
	About Symantec DLP Agent Installation .....	1102
	What gets installed for Symantec DLP Agents .....	1103
	About preinstallation steps for Symantec DLP Agents .....	1104
	About Symantec DLP Agent security .....	1105
	About the watchdog service .....	1107
	About Endpoint Server redundancy .....	1108
	About the AgentInstall.msi package .....	1108
	Installing Symantec DLP Agents with the Symantec Management Console .....	1111

	Installing Symantec DLP Agents with an unattended installation .....	1112
	Installing Symantec DLP Agents manually .....	1114
	Installing the Symantec DLP Agent on FIPS-compliant computers .....	1116
Chapter 69	Managing Symantec DLP Agents .....	1117
	About Symantec DLP Agent administration .....	1117
	Using the agents overview screen .....	1117
	Agent management events screen .....	1124
	About Symantec DLP Agent removal .....	1126
Chapter 70	About application monitoring .....	1131
	About application monitoring .....	1131
	Adding an application .....	1132
Chapter 71	Using Endpoint Server tools .....	1135
	About Endpoint tools .....	1135
	Using Endpoint tools with Windows 7 or Vista .....	1136
	About endpointkeytool utility .....	1136
	Shutting down the agent and the watchdog services .....	1138
	Inspecting the database files accessed by the agent .....	1139
	Viewing extended log files .....	1140
	About the Device ID utility .....	1140
Index	.....	1143

# 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](#)



# 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 Endpoint Discover](#)
- [About Endpoint Prevent](#)
- [About Data Classification for Enterprise Vault](#)

## About Symantec Data Loss Prevention

Symantec Data Loss Prevention enables you to:

- Discover and locate confidential information on file and Web servers, in databases, and on endpoints (desk and laptop systems)
- Protect confidential information through quarantine
- Monitor network traffic for transmission of confidential data
- Monitor the use of sensitive data on endpoint computers
- 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 37.
  - See [“About Symantec Data Loss Prevention administration”](#) on page 45.
  - See [“About the Enforce Server administration console”](#) on page 46.
- **Network Discover**
  - See [“About Network Discover”](#) on page 39.
- **Network Protect**
  - See [“About Network Protect”](#) on page 40.
- **Network Monitor**
- **Network Prevent**
- **Endpoint Discover**
  - See [“About Endpoint Discover”](#) on page 40.
  - See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.
- **Endpoint Prevent**
  - See [“About Endpoint Prevent”](#) on page 41.
- **Symantec Data Classification for Enterprise Vault**
  - See [“About Data Classification for Enterprise Vault”](#) on page 41.

The Discover, Protect, 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 quarantines sensitive data on file servers, as specified in your policies.

See [“About Network Discover”](#) on page 39.

- Network Monitor Server monitors the traffic on your network.

See [“About Network Monitor and Prevent”](#) on page 38.

- Network Prevent (Email) Server blocks emails that contain sensitive data.

See [“Implementing Network Prevent \(Email\)”](#) on page 813.

- Network Prevent (Web) Server blocks HTTP postings and FTP transfers that contain sensitive data.

See [“Implementing Network Prevent \(Web\)”](#) on page 827.

- Endpoint Server monitors and prevents the misuse of confidential data on endpoint computers.

See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.

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 35.

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 policies”](#) on page 307.

See [“Introduction to policy detection”](#) on page 281.

- 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 745.
- 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 783.  
See [“Remediating incidents”](#) on page 787.
- 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 77.

## 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.  
See [“Implementing Network Monitor”](#) on page 803.
- **Network Prevent (Email)**  
Network Prevent (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 (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 (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 (Email).

See [“Implementing Network Prevent \(Email\)”](#) on page 813.

See the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)*.

- Network Prevent (Web)

For in-line active Web request management, Network Prevent (Web) integrates with an HTTP, HTTPS, or FTP proxy server. This integration uses the Internet Content Adaptation Protocol (ICAP). The Network Prevent (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.

See [“Implementing Network Prevent \(Web\)”](#) on page 827.

## 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 35.

See [“About Network Discover”](#) on page 843.

## 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 35.

See [“Configuring Network Protect for file shares”](#) on page 906.

## About Endpoint Discover

Endpoint Discover detects sensitive data on your desktop or your laptop endpoint computers. It consists of at least one Endpoint Server and at least one Symantec DLP Agent that runs on an endpoint computer. 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 Endpoint Discover and Endpoint Prevent”](#) on page 1049.

See [“About Symantec Data Loss Prevention”](#) on page 35.

## About Endpoint Prevent

Endpoint Prevent detects and prevents sensitive data from leaving from your desktop or your laptop endpoint computers. 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:

- Removable media devices
- IM
- HTTP/HTTPS
- Email/SMTP
- FTP
- Network shares
- CD/DVD
- Print/Fax
- Clipboard
- Application monitoring

See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.

See [“About Symantec Data Loss Prevention”](#) on page 35.

## About Data Classification for Enterprise Vault

Symantec Data Classification for Enterprise Vault uses Symantec Data Loss Prevention detection technologies to automate the classification of Microsoft Exchange messages that are managed in Symantec Enterprise Vault for Microsoft Exchange. The Discovery Accelerator and Compliance Accelerator, which are available separately from the Data Classification for Enterprise Vault solution, can use classification tags to filter messages during searches or audits.

The Data Classification for Enterprise Vault solution uses these components:

- Symantec Enterprise Vault for Microsoft Exchange—Provides the framework for archiving Microsoft Exchange messages.
- Data Classification for Enterprise Vault filter—Works with Symantec Enterprise Vault for Microsoft Exchange to post Exchange messages to a Classification Server, and to receive the message classification result from the Classification Server. Symantec Enterprise Vault for Microsoft Exchange then uses the classification result to delete or to archive and classify the message.
- Classification Server—The Classification Server is a new type of Symantec Data Loss Prevention detection server that receives messages from the Data Classification for Enterprise Vault filter and applies policies to the messages to generate classification results. The Classification Server is able to evaluate Exchange messages using any of the available Symantec Data Loss Prevention detection technologies, including EDM, IDM, and DCM. The server can also use a new classification-specific detection rule that evaluates Exchange messages based on their message attributes (MAPI attributes).  
The Classification Server is installed and registered in the same way as other Symantec Data Loss Prevention detection servers. See the *Symantec Data Loss Prevention Installation Guide* for your platform for more information.
- Classification policies—Instead of generating a Symantec Data Loss Prevention incident, classification policies use the **Classify Enterprise Vault Content** response rule action to generate a classification result and return that result to the Data Classification for Enterprise Vault filter. The response rule configuration indicates whether the classification result should instruct Enterprise Vault to archive or delete the message. For archived messages, the response rule also specifies the retention category and classification tag that should be assigned to the message. The rule also determines whether or not Enterprise Vault for Microsoft Exchange should include archived messages in compliance reviews or exclude them for further review. For messages that are not archived, the response rule specifies the method that Enterprise Vault for Microsoft Exchange should use to delete those messages.

---

**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 Exchange Agent filter and Classification Server to communicate with one another. See the *Symantec Enterprise Vault Data Classification Services Implementation Guide* for more information.

---

Classification policies are configured using the same Enforce Server administration console pages that you use to configure Symantec Data Loss Prevention policies.

However, the MAPI detection rule and the classification response action are applicable only if you have licensed a Classification Server.



# 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 46.

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 48.

## 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 **Home** screen is displayed. 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:

**Table 2-1** Administration console navigation and operation icons

Icon	Description
	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.
	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.
	Send the current report to the printer. If the current screen contents cannot be sent to the printer, this icon is unavailable.

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

Icon	Description
	Email the current report to one or more recipients. If the current screen contents cannot be sent as an email, this icon is unavailable.

See “[Logging on and off the Enforce Server administration console](#)” on page 47.

## 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

- 1 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).
- 2 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 82.

- 3 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*.

- 4 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 50.

See [“Logging on and off the Enforce Server administration console”](#) on page 47.

## 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 49.

See [“Adding an administrator email account”](#) on page 50.

## 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 48.
- Add and configure your detection servers.  
See [“Adding a detection server”](#) on page 166.  
See [“Server configuration—basic”](#) on page 152.
- 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 policies 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 89.

### To change the administrator password

- 1 Log on as administrator.
- 2 Take one of the following actions:
  - Click **profile** in the upper-right corner of the administration console.
  - Go to **Administration > Users > Users** and click on the administrator user. The **Configure User** screen is displayed.
- 3 On the **Configure User** screen:
  - Enter your current (old) password in the **Old Password** field.
  - 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.

- 4 Click **Save**.

See “[About the administrator account](#)” on page 48.

See “[About the Enforce Server administration console](#)” on page 46.

See “[About the System Overview screen](#)” on page 169.

## 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

- 1 Go to **Administration > Users > Users** and click on the administrator user.
- 2 On the Edit Profile screen that appears, type the administrator password in the **Old Password** field.
- 3 Type the new (or changed) administrator email address in the **email Address** field.

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

- 4 Click **Save**.

See [“About the administrator account”](#) on page 48.

See [“About the Enforce Server administration console”](#) on page 46.

See [“About the System Overview screen”](#) on page 169.

## 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**

- 1 Enter your current valid password in the **Old Password** field.
- 2 Enter your new password in the **New Password** field.
- 3 Re-enter your new password in the **Re-enter New Password** field.
- 4 Click **Save**.

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

See [“Changing your password”](#) on page 53.

**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**

- 1 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 55.

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 60.

- **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 59.

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.
- 3 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**

- 1 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.

**To select XML export details**

- 1 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.
- 3 **Include Incident History in XML Export.** If this box is checked, reports exported to XML include the incident history data that is contained in the **History** tab of each incident snapshot.
- 4 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.

## 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

- 1 Enter your old password in the **Old password** field of the **Password Renewal** window.
- 2 Enter your new password in the **New Password** field of the **Password Renewal** window.
- 3 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 50.

See [“About the administrator account”](#) on page 48.

See [“Logging on and off the Enforce Server administration console”](#) on page 47.



# 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 [Table 3-1](#) on page 56.
- 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 58.
- Locale-based date and number formats, as well as sort orders for lists and reports.  
 See [“About locales”](#) on page 60.
- 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 9.x	Version 10.0	Version 10.5	Version 11.0
Arabic		Yes	Yes	Yes
Brazilian Portuguese		Yes	Yes	Yes
Chinese (traditional)	Yes	Yes	Yes	Yes
Chinese (simplified)	Yes	Yes	Yes	Yes
Czech		Yes	Yes	Yes
Danish	Yes	Yes	Yes	Yes
Dutch	Yes	Yes	Yes	Yes
English	Yes	Yes	Yes	Yes
Finnish	Yes	Yes	Yes	Yes

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

Language	Version 9.x	Version 10.0	Version 10.5	Version 11.0
French	Yes	Yes	Yes	Yes
German	Yes	Yes	Yes	Yes
Greek		Yes	Yes	Yes
Hebrew	Yes	Yes	Yes	Yes
Hungarian		Yes	Yes	Yes
Italian	Yes	Yes	Yes	Yes
Japanese	Yes	Yes	Yes	Yes
Korean	Yes	Yes	Yes	Yes
Norwegian	Yes	Yes	Yes	Yes
Polish		Yes	Yes	Yes
Portuguese	Yes	Yes	Yes	Yes
Romanian		Yes	Yes	Yes
Russian	Yes	Yes	Yes	Yes
Spanish	Yes	Yes	Yes	Yes
Swedish	Yes	Yes	Yes	Yes
Turkish		Yes*	Yes*	Yes*

\*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.

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

A number of capabilities are not implied by this support:

- 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.
- 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 55.

## 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 55.

## 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 61.

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 60.

See “[About support for character sets, languages, and locales](#)” on page 55.

## 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://java.sun.com/j2se/version/docs/guide/intl/locale.doc.html>, where *version* equals the currently supported Java version.

Any locales listed as "fully supported locales" or as "also provided, but not tested" may be used except Turkish. English is the default locale, so it need not be independently selected.

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 61.

See “[About support for character sets, languages, and locales](#)” on page 55.

# 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 59.

See [“About locales”](#) on page 60.

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

- 1 On the Enforce Server, go to **System > Settings > General** and click **Configure**. The **Edit General Settings** screen is displayed.
- 2 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.
- 3 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 50.

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

See [“Using the Language Pack Utility”](#) on page 62.

See [“About support for character sets, languages, and locales”](#) on page 55.

## 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 `\Vontu\Protect\bin` directory.

To use the Language Pack Utility, you must have Read, Write, and Execute permissions on all of the `\Vontu` 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 `VontuIncidentPersister` 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.

---

### To add a language pack

- 1 Advise other users that anyone currently using the Enforce Server administration console must save their work and log off.
- 2 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_10.5_Lang_Pack-JP.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_10.5_Lang_Pack-TW.zip  
Symantec_DLP_10.5_Lang_Pack-CS.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**.

Language packs for Symantec Data Loss Prevention can be obtained from Symantec [File Connect](#).

### To remove a language pack

- 1 Advise users that anyone currently using the Enforce Server administration console must save their work and log off.
- 2 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**

- 1 Advise users that anyone currently using the Enforce Server administration console must save their work and log off.
- 2 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
```

- 3 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 55.



# Managing the Enforce Server platform

- [Chapter 4. Managing Enforce Server services and settings](#)
- [Chapter 5. Managing roles and users](#)
- [Chapter 6. Managing stored credentials](#)
- [Chapter 7. Managing system events and messages](#)
- [Chapter 8. Adding a new product module](#)
- [Chapter 9. Migrating Symantec Data Loss Prevention servers to 64-bit operating systems](#)



# Managing Enforce Server services and settings

This chapter includes the following topics:

- [About Enforce Server services](#)
- [About starting and stopping services on Windows](#)
- [Starting and stopping services on Linux](#)

## About Enforce Server 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** Services on the Enforce Server

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. This service only runs during system updates and upgrades.

See [“About starting and stopping services on Windows”](#) on page 70.

## 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 70.
- See [“Stopping an Enforce Server on Windows”](#) on page 70.
- See [“Starting a Detection Server on Windows”](#) on page 71.
- See [“Stopping a Detection Server on Windows”](#) on page 71.
- See [“Starting services on single-tier Windows installations”](#) on page 72.
- See [“Stopping services on single-tier Windows installations”](#) on page 72.

## 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

- 1 On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
- 2 Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
- 3 Start the remaining Symantec Data Loss Prevention services, including the following services:
  - Vontu Manager
  - Vontu Incident Persister
  - Vontu Update
  - Vontu Monitor Controller

See [“Stopping an Enforce Server on Windows”](#) on page 70.

## 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

- 1 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, which might include the following services:
  - Vontu Update
  - Vontu Incident Persister
  - Vontu Manager
  - Vontu Monitor Controller
  - Vontu Notifier

See [“Starting an Enforce Server on Windows”](#) on page 70.

## Starting a Detection Server on Windows

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

- 1 On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
- 2 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 71.

## 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

- 1 On the computer that hosts the detection 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, which might include the following services:

- Vontu Update
- Vontu Monitor

See [“Starting a Detection Server on Windows”](#) on page 71.

## 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

- 1 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 Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
- 3 Start the remaining Symantec Data Loss Prevention services, which might include the following services:
  - Vontu Manager
  - Vontu Monitor
  - Vontu Incident Persister
  - Vontu Update
  - Vontu Monitor Controller

See [“Stopping services on single-tier Windows installations”](#) on page 72.

## 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

- 1 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 From the Services menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
  - Vontu Update

- Vontu Incident Persister
- Vontu Manager
- Vontu Monitor Controller
- Vontu Notifier
- Vontu Monitor

See [“Starting services on single-tier Windows installations”](#) on page 72.

## 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 73.
- See [“Stopping an Enforce Server on Linux”](#) on page 74.
- See [“Starting a detection server on Linux”](#) on page 74.
- See [“Stopping a detection server on Linux”](#) on page 74.
- See [“Starting services on single-tier Linux installations”](#) on page 75.
- See [“Stopping services on single-tier Linux installations”](#) on page 75.

## 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/Vontu/Protect/bin`.
- 3 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 74.

## 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 database, log on as root.
- 2 Change directory to `/opt/Vontu/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 73.

## 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 Enforce Server, log on as root.
- 2 Change directory to `/opt/Vontu/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 74.

## 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**

- 1 On the computer that hosts the database, log on as root.
- 2 Change directory to `/opt/Vontu/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 74.

## 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**

- 1 On the computer that hosts the Symantec Data Loss Prevention server applications, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 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 75.

## 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/Vontu/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 75.

# Managing roles and users

This chapter includes the following topics:

- [About role-based access control](#)
- [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](#)
- [Manage and add roles](#)
- [Manage and add users](#)
- [Integrating Active Directory for user 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 > User 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 [“About policy deployment”](#) on page 312.

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`

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 48.

## 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 48.

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 79.
- 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 80.

- If necessary, modify the solution-pack roles and create any required new roles. See [“Configuring roles”](#) on page 82.
- Create users and assign each of them to one or more roles. See [“Configuring user accounts”](#) on page 89.
- Manage roles and users and remove those not being used. See [“Manage and add roles”](#) on page 91. See [“Manage and add users”](#) on page 92.

## 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 Administrator**  
 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 remediate 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 80.

## 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 5-1](#) on page 81.

**Table 5-1** Financial Services Solution Pack roles

Role Name	Description
<b>Compliance</b>	<p>Compliance Officer:</p> <ul style="list-style-type: none"> <li>■ Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.</li> <li>■ 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.</li> </ul>
<b>Exec</b>	<p>Executive:</p> <ul style="list-style-type: none"> <li>■ Users in this role can view, remediate, and delete incidents; look up attributes; and view all custom attributes.</li> <li>■ 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.</li> </ul>
<b>HRM</b>	<p>HR Manager:</p> <ul style="list-style-type: none"> <li>■ Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.</li> <li>■ This role provides users with access privileges to respond to the security incidents that are related to employee breaches.</li> </ul>
<b>Investigator</b>	<p>Incident Investigator:</p> <ul style="list-style-type: none"> <li>■ Users in this role can view, remediate, and delete incidents; look up attributes; and edit all custom attributes.</li> <li>■ 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.</li> </ul>
<b>ISM</b>	<p>InfoSec Manager:</p> <ul style="list-style-type: none"> <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>

**Table 5-1** Financial Services Solution Pack roles (*continued*)

Role Name	Description
<b>ISR</b>	<p>InfoSec Responder:</p> <ul style="list-style-type: none"> <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>
<b>Report</b>	<p>Reporting and Policy Authoring:</p> <ul style="list-style-type: none"> <li>■ Users in this role can view and remediate incidents, and author all policies and policy groups. They have no access to incident details.</li> <li>■ This role provides a single role for policy authoring and data loss risk management.</li> </ul>
<b>Sys Admin</b>	<p>System administrator:</p> <ul style="list-style-type: none"> <li>■ Users in this role can administer the system and the system users, and can view incidents. They have no access to incident details.</li> </ul>

## 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 77.

See [“About configuring roles and users”](#) on page 78.

### To configure a role

- 1 Navigate to the **System > User 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):

**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) and Indexed Document Matching (IDM).
- Configure and assign incident attributes.
- Configure system settings.
- Configure response rules.
- Create policy groups.
- Configure recognition protocols.
- View system event and traffic reports.

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

- In the **Incidents** section, you grant users in this role the following incident privilege(s):

### 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 three types of incidents: **Network Incidents**, **Discover Incidents**, and **Endpoint Incidents**.
- 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, and execute response rule actions.

**■ Lookup Attributes**

Lets users view the attributes of an incident.

**■ Delete Incidents**

Lets users delete an incident.

**■ Export Web Archive**

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

**■ XML Export**

Lets users export a report of incidents in XML format.

**■ CSV Attachment in Email Reports**

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

**■ Reporting API**

This privilege gives users the right to access the Reporting API Web Service. The Reporting API enables clients to retrieve incident data from the Enforce Server by using SOAP requests and responses. Each client that accesses the Reporting API Web Service must authenticate as an Enforce Server user and have the **Reporting API** privilege. See the *Symantec Data Loss Prevention Reporting 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.

**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 values.
- To restrict the users to certain custom attributes, clear the **Edit All** check box and individually select the **Edit** check box for each custom attribute you want 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**.

---

**Note:** These settings apply to all incident reports in the system. These reports include the Executive Summary, Incident Summary, Incident List, and Incident Snapshots.

---

---

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

---

- 4 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.

---

- 6 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:

- 1 In the Enforce Server Administration Console, go to the **System > User Management > Users**.
- 2 Click **Add User**.
- 3 Enter the user name in the **Name** field.
  - The user name must be between 8 and 30 characters long, is case sensitive, and cannot contain backslashes (\).
- 4 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 90.
  - If you configure Active Directory integration with the Enforce Server, users can authenticate using their Active Directory passwords. In this case the password field does not appear in the **Users** screen. See [“Integrating Active Directory for user authentication”](#) on page 92.
- 5 Optionally you can enter an **Email Address** for the user.
- 6 You can intentionally lock a user out of the system by selecting the **Account Disabled** box.
  - 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.

- 7 Depending on the language pack(s) you have installed, you can set the language preference for the user.
- 8 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.
- 9 Select the roles to assign data and incident access privileges to the user.
  - A user must be assigned to a role. If no role has been created the user is assigned to the default role.See [“Configuring roles”](#) on page 82.
- 10 Click **Save** to save the user configuration.

---

**Note:** Once you have saved the new user, the user name cannot be edited.

---

- 11 Manage users and roles as necessary.
  - See [“Manage and add roles”](#) on page 91.
  - See [“Manage and add users”](#) on page 92.

## 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 92.

### 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.

- 3 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).

## Manage and add roles

The **System > User 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 82.
- 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 92.

## Manage and add users

The **System > User Management > 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 89.
- 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 91.

## 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

- 1 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.

---

- 2 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 93.

- 3 Confirm that the Enforce Server can communicate with the Active Directory server.

See [“Verifying the Active Directory connection”](#) on page 95.

- 4 Configure Symantec Data Loss Prevention to use Active Directory authentication.

See [“Configuring the Enforce Server for Active Directory authentication”](#) on page 96.

## 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 `Vontu_home\Protect\config` (for example, `c:\Vontu\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
    }
    QA.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 `engAD.eng.company.com`.

**To create the `krb5.ini` or `krb5.conf` file**

- 1 Go to `Vontu_home\Protect\config` and locate the sample `krb5.ini` file. For example, locate the file in `c:\Vontu\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 95.
- 3 Open the `krb5.ini` or `krb5.conf` file in a text editor.
- 4 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
```

- 5 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`.
- 6 Replace the sample `kdc` values with the hostnames 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.
- 7 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.
- 8 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. Symantec Data Loss Prevention ships with the `kinit` utility stored in `c:\Vontu\jre\bin` (on Windows) or `/opt/Vontu/jre/bin` (on Linux). 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 96.

#### To test the connection to the Active Directory server

- 1 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.

- 3 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 92.

**To configure the Enforce Server to use 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).
- 3 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.

- 4 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`.

- 6 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 93.

- 7 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.



# 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 100.

See [“Managing credentials in the credential store”](#) on page 101.

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 855.

## 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:

<b>Credential Name</b>	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.
<b>Access Username</b>	Enter the user name for authentication.
<b>Access Password</b>	Enter the password for authentication.
<b>Re-enter Access Password</b>	Re-enter the password.

- 3 Click **Save**.
- 4 You can later edit or delete credentials from the credential store.  
See [“Managing credentials in the credential store”](#) on page 101.  
See [“Configuring endpoint credentials”](#) on page 100.

## 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 endpoint computers that are connected to an Endpoint Server. Because all endpoint computers 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**.
- 6 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**.
- 9 Click **Save**.

See [“About the credential store”](#) on page 99.

See [“Configuring the Endpoint Discover: Quarantine File action”](#) on page 722.

## Managing credentials in the credential store

You can delete or edit a stored credential.

### To delete a stored credential

- 1 Click **System > Settings > Credentials**. Locate the name of the stored credential that you want to remove.
- 2 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

- 1 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.
- 3 Update the user name or password.
- 4 Click **Save**.
- 5 If you change the password for a given credential, the new password is used for all subsequent Discover scans that use that credential.



# 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 169.
- Reports on all system events of any severity can be viewed by going to **System > Servers > Events**. See [“System events reports”](#) on page 104.
- Recent system events for a particular detection server are listed on the **Server Detail** screen for that server. See [“Server Detail screen”](#) on page 172.
- 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 108.

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 115.
- Syslog functionality  
See [“Enabling a syslog server”](#) on page 113.

Some system events require a response.

See [“About system event responses”](#) on page 111.

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 104.
- Configure the system event thresholds for individual servers.  
See [“Configuring event thresholds and triggers”](#) on page 109.

## 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 7-1** System events list

Type	The type (severity) of the event. Type may be any one of those listed in <a href="#">Table 7-2</a> .
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 <a href="#">“System event codes and messages”</a> on page 119.
Summary	A brief description of the event. Click on the summary for more detail about the event.

**Table 7-2** System event types

-  System information
-  Warning
-  Severe

You can select from several report handling options.

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 108.

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**

- 1** 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**

- 1** 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 7-3](#).
- 4** 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.
- 6** (Optional) Specify additional advanced filters if needed.
- 7** 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 7-3** System events advanced filter options

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

---

**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 or Professional Services. 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 109.

---

See [“About system events”](#) on page 103.

See [“Server event detail”](#) on page 108.

See [“Working with saved system reports”](#) on page 107.

See [“Configuring event thresholds and triggers”](#) on page 109.

See [“About system alerts”](#) on page 115.

## 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 46.
- 2 Select the filters and summaries for your custom report.  
See [“About custom reports and dashboards”](#) on page 753.
- 3 Select **Report > Save As**.
- 4 Enter the saved report information.  
See [“Saving custom incident reports”](#) on page 755.
- 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 users 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 755.
- 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 755.
- 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 104.

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**.

**Table 7-4** Event detail — General

Type	The event is one of the following types: <ul style="list-style-type: none"><li>■ Info: Information about the system.</li><li>■ Warning: A problem that is not severe enough to generate an error.</li><li>■ Severe: An error that requires immediate attention.</li></ul>
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 7-5** Event detail — Message

Code	A number that identifies the kind of event. See <a href="#">“System event codes and messages”</a> on page 119.
------	---

**Table 7-5** Event detail — Message (*continued*)

Summary	A brief description of the event.
Detail	Detailed information about the event.

See “[About system events](#)” on page 103.

See “[Server event detail](#)” on page 108.

See “[System events reports](#)” on page 104.

See “[About system alerts](#)” on page 115.

## 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 or Professional Services. 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 103.

**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 7-6** 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.	<i>process name</i> 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
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

**Table 7-6** Configurable parameters that trigger events (*continued*)

Parameter	Description	Event
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 slowed down or stopped. The default is 10000.	$N$ 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
- System alert email messages  
See “[About system alerts](#)” on page 115.
- Syslog functionality  
See “[Enabling a syslog server](#)” on page 113.

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.

**Table 7-7** System event responses

System Event or Category	Appropriate Response
Low disk space	<p>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.</p> <p>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.</p>
Tablespace is almost full	<p>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.</p> <p>Refer to the <i>Symantec Data Loss Prevention Installation Guide</i>.</p>
Licensing and versioning	Contact Symantec Support.
Monitor not responding	<p>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.</p> <p>See <a href="#">“About Enforce Server services”</a> on page 69.</p>
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.
Cryptographic keys are inconsistent	Contact Symantec Support.

**Table 7-7** System event responses (*continued*)

System Event or Category	Appropriate Response
Long message wait time	<p>Increase detection server capacity by adding more CPUs or replacing the computer with a more powerful one.</p> <p>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.</p> <p>Increase the threshold wait times if all of the following items are true:</p> <ul style="list-style-type: none"> <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 message processing.</li> </ul>
process_name restarts excessively	<p>Check the process by going to <b>System &gt; Servers &gt; 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>.</p>
N incidents in queue	<p>Investigate the reason for the incidents filling up the queue.</p> <p>The most likely reasons are as follows:</p> <ul style="list-style-type: none"> <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

- 1 Go to the `\Vontu\Protect\config` directory on Windows or the `/opt/Vontu/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.
- 4 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%.
```

---

**Note:** Be sure to comment out the `#systemevent.syslog.format= [{0}] {1} - {2}` line. Do not comment out the `#systemevent.jmx.format= [{0}] {1} - {2}` line. The `jmx` option is not compatible with syslog servers.

---

See [“About system events”](#) on page 103.

## 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 115.

See [“Configuring system alerts”](#) on page 117.

See [“Server event detail”](#) on page 108.

## 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.

**2** 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.
- 3 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.

- 4 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.

- 5 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.

- 6 Click **Save**.

See [“About system alerts”](#) on page 115.

See [“Configuring system alerts”](#) on page 117.

See “[About system events](#)” on page 103.

## 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 115.

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 115.

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 to 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.

- 6 Enter the email address that the alert is to be sent to. Separate multiple addresses by commas.

- 7 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.

- 8 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 119.

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 115.

See [“Configuring the Enforce Server to send email alerts”](#) on page 115.

See [“System events reports”](#) on page 104.

## 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: `\Protect\logs`
- Linux: `/var/log/Vontu`

See [“About log files”](#) on page 225.

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 different event is identified by code number listed in the following table.

See [“About system events”](#) on page 103.

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

See [“System events reports”](#) on page 104.

Note that numbers enclosed in braces, such as {0}, indicate where appropriate text strings are inserted in the actual message.

Code	Name	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.

Code	Name	Description
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.
1014	Low disk space	Hard disk space is low. Symantec Data Loss Prevention server disk usage is over {0}%.
1100	Aggregator started	
1101	Aggregator failed to start	Error starting Aggregator. {0} No incidents will be detected.
1200	Loaded policy	"{0}" Policy "{0}" v{1} ({2}) has been successfully loaded.
1201	Loaded policies {0}	
1202	No policies loaded	No relevant policies are found. No incidents will be detected. 1203 Unloaded policy "{0}" Policy "{0}" has been unloaded.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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}.
1301	File Reader started	
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}.

Code	Name	Description
1400	ICAP channel configured	<p>The channel is in {0} mode The current configuration values are:</p> <p>REQMOD Filtering: Ignore requests smaller than: {1}</p> <p>Ignore requests without attachments filter is {2} Ignore requests to hosts or domains filter: {3}</p> <p>Ignore requests from user-agents filter: {4}</p> <p>RESPMOD Filtering: Ignore responses smaller than: {5}</p> <p>Inspect Content Type: {6}</p> <p>Ignore responses from hosts or domains filter: {7}</p> <p>Ignore responses to user-agents filter: {8}</p> <p>Connection: Bind Address is {9}</p> <p>ICAP port is {10}</p> <p>Maximum number of connections for REQMOD is {11} and RESPMOD is {12}</p> <p>Connection backlog is {13} Proxy white list includes: {14}.</p>
1401	Invalid license	<p>The ICAP channel is not licensed or the license has expired. No incidents will be detected or prevented by the ICAP channel.</p>
1402	Content Removal Incorrect	<p>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.</p>
1403	Out of memory Error (Web Prevent) while processing message	<p>While processing request on connection ID{0}, out of memory error occurred. Please tune your setup for traffic load.</p>

<b>Code</b>	<b>Name</b>	<b>Description</b>
1404	Host restriction	Any host (ICAP client) can connect to Web Prevent.
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 Traces available at {0} 1408 Invalid Load Balance Factor Icap.LoadBalanceFactor configured to 0. Treating it as 1.
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.
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.
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}

<b>Code</b>	<b>Name</b>	<b>Description</b>
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}
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}.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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}%.
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.
2000	Key ignition error	Failed to ignite keys with the new ignition password. Detection against Exact Data Profiles will be disabled.
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.
2100	Administrator saved	The administrator settings were successfully saved.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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.
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}

<b>Code</b>	<b>Name</b>	<b>Description</b>
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.
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	
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.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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.
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.
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}.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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.
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.
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}.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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		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.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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}".
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.
2600	Communication error	Unexpected error occurred while sending {1} updates to {0}. {2} Please look at the monitor controller logs for more information.
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}.
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}.
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}	
2900	EDM profile search failed {0}	

<b>Code</b>	<b>Name</b>	<b>Description</b>
2901	Keys are not ignited	Exact Data Matching will be disabled until the cryptographic keys are ignited.
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	{0} {1} Exact data profile was not created.	
2906	Indexing canceled	Creation of database profile {0} was canceled.
2907	Replication canceled	Canceled replication of database profile {0} to server {1}.
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.

<b>Code</b>	<b>Name</b>	<b>Description</b>
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}.
2920	Failed to load database profile {1}	No incidents will be detected against database profile {0}.
2921	Failed to unload database profile {1}	It may not be possible to reload the database profile {0} in the future without monitor restart.
2922	could not find registered content	Registered content with ID {0} was not found in database during indexing.
2923	Database error	Database error occurred during indexing. {0}
2924	Process shutdown during indexing	The process has been shut down 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}". Rows processed: {2} Invalid rows: {3} The exact data profile will now be replicated to all Symantec Data Loss Prevention Servers.
3000	{0} {1}	Document profile was not created.

<b>Code</b>	<b>Name</b>	<b>Description</b>
3001	Indexing canceled	Creation of document profile {0} was canceled.
3002	Replication canceled	Canceled replication of document profile {0} to server {1}.
3003	Replication failed	Connection to database was lost while replicating document profile {0} to server {1}.
3004	Replication failed	Database error occurred while replicating document profile {0} to server {1}.
3005	Failed to remove index file	Failed to delete index file {1} of document profile {0}.
3006	Failed to remove index files	Failed to delete index files {1} of document profile {0}.
3007	Failed to remove orphaned file {0}	
3008	Replication failed	Replication of document profile {0} to server {2} failed. {1} Check the monitor controller log for more details.
3009	Replication completed	Completed replication of document profile {0} to server {2}. File {1} was transferred successfully.
3010	Replication completed	

# 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 `name.slf`.

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.

- 4 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.

---

- 5 To enable full functionality of new product license-related features, restart the Vontu Manager Service.

See “[About Enforce Server services](#)” on page 69.

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 45.

# Migrating Symantec Data Loss Prevention servers to 64-bit operating systems

This chapter includes the following topics:

- [Migrating Symantec Data Loss Prevention servers from 32-bit to 64-bit operating systems](#)
- [Migrating the Enforce Server to a 64-bit operating system](#)
- [Migrating a detection server to a 64-bit operating system](#)

## Migrating Symantec Data Loss Prevention servers from 32-bit to 64-bit operating systems

Symantec Data Loss Prevention supports running the Enforce Server and detection servers on 64-bit operating systems. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about supported 64-bit operating systems and server hardware configurations. This section describes the steps that are required to migrate an existing 32-bit Symantec Data Loss Prevention server to a supported 64-bit operating system on a separate server computer or virtual machine (if VM deployments are supported for the server).

Before you begin the migration process, consider these important restrictions and requirements:

- All components of the Symantec Data Loss Prevention deployment—the Enforce Server, Enforce Server database, and all detection servers—must be fully upgraded to the latest Symantec Data Loss Prevention version before you begin

the migration process. The migration process is separate from the Symantec Data Loss Prevention upgrade process, and you can only migrate servers that are already at the latest version. Do not attempt to migrate a 32-bit, version 10.x component to 64-bit.

- Migrating servers to a 64-bit operating system is not an automated process. You must install new 64-bit Symantec Data Loss Prevention server software on a compatible 64-bit operating system, and then re-use, re-create, or migrate supporting files from the 32-bit Symantec Data Loss Prevention server. Migrating a server “in place” is not possible.
- Cross-platform migrations are not supported. For each Symantec Data Loss Prevention server that you migrate, the target 64-bit operating system must be of the same type (Windows or Linux) as the existing 32-bit operating system.
- Certain Symantec Data Loss Prevention products may have limited functionality when deployed on 64-bit operating systems. For example, Network Discover does not support native Lotus Notes scanning on 64-bit platforms. Also, any FlexResponse plug-ins that use native code must be recompiled to support the 64-bit operating system. Review the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* to ensure that all required Symantec Data Loss Prevention features and third-party utilities are available on the target 64-bit platform.
- You can migrate the Enforce Server independently of the Oracle database that stores the Enforce Server database, and vice versa. If you intend to migrate the Oracle database server to 64-bit, Symantec recommends that you migrate Oracle before migrating the Enforce Server. By migrating Oracle first, you avoid having to reconfigure the Enforce Server to access a new Oracle database after migration.
- You can migrate detection servers independently of the Enforce Server, and vice versa.
- A 32-bit Enforce Server, Oracle database server, or detection servers can operate alongside 64-bit Symantec Data Loss Prevention servers or Oracle database servers. You do not have to upgrade all components of your Symantec Data Loss Prevention deployment to 64-bit.

During the migration process, you use several procedures that are described in other Symantec Data Loss Prevention documents. For example, if you want to migrate the Enforce Server database to a 64-bit platform, you use the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* both to upgrade the database software to Oracle 11g and then migrate software and database to a 64-bit platform.. The migration instructions direct you to the correct guides and procedures when necessary.

**Table 9-1** Migrating Symantec Data Loss Prevention servers from 32-bit to 64-bit operating systems

Phase	Action	Description
Phase 1	Upgrade all Symantec Data Loss Prevention servers to the latest version.	<p>The existing Enforce Server and all detection servers must be at the latest version before you begin the migration process.</p> <p>See the <i>Symantec Data Loss Prevention Upgrade Guide</i> for your platform.</p>
Phase 2	Back up your Enforce Server database.	See the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i> .
Phase 3	(Optional) Migrate the Enforce Server database to a 64-bit operating system.	<p>To migrate an existing Enforce Server database to 64-bit, you must first upgrade the database software to Oracle 11g. You can then migrate the Enforce Server database to a new 64-bit server computer or virtual machine.</p> <p>See the chapter “Migrating from 32-bit Oracle 10g to 64-bit Oracle 11g” in the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i>.</p>
Phase 4	Stop all Network Discover scans before you begin migrating either the Enforce Server or a Network Discover detection server.	<p>See <a href="#">“Managing Network Discover target scans”</a> on page 874.</p> <p>Do not restart scans until you have finished migrating the server.</p>
Phase 5	(Optional) Migrate the Enforce Server.	See <a href="#">“Migrating the Enforce Server to a 64-bit operating system”</a> on page 140.

**Table 9-1** Migrating Symantec Data Loss Prevention servers from 32-bit to 64-bit operating systems (*continued*)

Phase	Action	Description
Phase 6	(Optional) Update the Symantec DLP Agent connectivity configuration on endpoint computers.	<p>If you intend to migrate an Endpoint Prevent detection server to a 64-bit system, ensure that the Symantec DLP Agents on all endpoint computers are configured to use an available, backup Endpoint Prevent detection server during the migration process.</p> <p>See <a href="#">“About Endpoint Server redundancy”</a> on page 1108.</p> <p>Alternatively, update all Symantec DLP Agents on endpoint computers to include the IP address of the new 64-bit server in their list of Endpoint Prevent servers. Making this configuration change now ensures that endpoint computers can automatically failover to the new 64-bit Endpoint Prevent server when it becomes available.</p>
Phase 7	(Optional) Migrate detection servers.	See <a href="#">“Migrating a detection server to a 64-bit operating system”</a> on page 143.

## Migrating the Enforce Server to a 64-bit operating system

Migrating the Enforce Server to a 64-bit operating system requires that you install a new 64-bit Enforce Server and preserve the existing Enforce Server database. Use the following procedure to ensure that all configuration data is preserved.

### To migrate the Enforce Server to a 64-bit operating system

- 1 Shut down the 32-bit Enforce Server and disable the services.  
See [“About starting and stopping services on Windows”](#) on page 70.  
See [“Starting and stopping services on Linux”](#) on page 73.
- 2 After you have verified that the services have stopped, disable the services to prevent them from automatically starting when the server computer reboots.
- 3 Install the 64-bit Enforce Server, making sure that you re-use (do not initialize) the existing Enforce Server database:
  - On the **Oracle Database Server Information** and **Oracle Database User Configuration** panels, enter the connectivity information and credentials for the existing Enforce Server database.
  - On the **Final Confirmation** panel, deselect the **Initialize Enforce Data** check box.

---

**Warning:** Do not initialize the Enforce Server database when you install the new 64-bit Enforce Server database. You must preserve the existing database to ensure that all configuration, policy, and incident data is carried over to the new system.

---

- After the installation completes, deselect the **Start Services** check box.
- See the *Symantec Data Loss Prevention Installation Guide* for your platform.

- 4 After installing the new 64-bit server, manually copy the following additional configuration files from the 32-bit server to the same directories on the 64-bit computer or virtual machine:

Directory	Description
<code>c:\Vontu\Protect\plugins</code> or <code>/opt/Vontu/Protect/plugins</code>	<p>Copy the entire contents of the <code>plugins</code> directory if you use custom plug-ins, or if you have configured native scan options with Network Discover.</p> <p>If you any plug-ins require resources that reside outside of the <code>plugins</code> directory, copy those resources as well.</p> <p><b>Note:</b> Any plug-ins that use native code must be recompiled for use on the 64-bit Enforce Server computer or virtual machine. Do not copy 32-bit native plugins to the new server.</p>
<code>c:\Vontu\Protect\config</code> or <code>/opt/Vontu/Protect/config</code>	<p>If you manually edited a Symantec Data Loss Prevention properties file (<code>.properties</code> extension) other than <code>jdbc.properties</code>, copy that file to the same location on the 64-bit Enforce Server computer or virtual machine.</p> <p><b>Note:</b> Do not copy the <code>jdbc.properties</code> file to the new server computer or virtual machine. Do not copy any configuration files (<code>.conf</code> extension) to the new computer.</p> <p>Many of the properties in these files define directory and file locations. If you copy a properties file to the 64-bit computer, also edit the file in its new location to ensure that all paths are valid. For example, if you installed the 32-bit Enforce Server on the <code>c:\</code> drive and the 64-bit server on the <code>d:\</code> drive, edit any copied properties files to specify <code>d:\</code> as the root drive.</p>
<code>c:\Vontu\Protect\scan\incremental_index</code> or <code>/var/Vontu/scan/incremental_index</code>	<p>If you configured Network Discover incremental scans, copy the entire <code>incremental_index</code> directory to the 64-bit Enforce Server installation to preserve the index data.</p>

---

**Note:** On Linux systems, ensure that you preserve the same file permissions and ownership attributes when copying files between systems.

---

- 5 Reinstall any language packs that you used on the 32-bit Enforce Server. See [“About Symantec Data Loss Prevention language packs”](#) on page 59.

- 6 Import any custom certificates that are necessary to communicate with installed detection servers, Active Directory connections, or FlexResponse plug-ins.  
See “Configuring certificates for secure communication” in the *Symantec Data Loss Prevention Installation Guide* for your platform.
- 7 Start the 64-bit Enforce Server after copying all configuration files.  
See “[About starting and stopping services on Windows](#)” on page 70.  
See “[Starting and stopping services on Linux](#)” on page 73.

## Migrating a detection server to a 64-bit operating system

To migrate a detection server follow these steps in order:

### To migrate a detection server to a 64-bit operating system

- 1 Ensure that the 64-bit detection server system contains all of the third-party software for the detection server you are migrating.  
For example, if you are migrating a 32-bit Network Discover detection server, you may also require a 64-bit version of Outlook 2010 on the server computer.
- 2 Install the 64-bit detection server software on the designated server computer or virtual machine (if the detection server supports virtual machine deployment).  
See the *Symantec Data Loss Prevention Installation Guide* for your platform.

- 3 After installing the new 64-bit server, manually copy the following additional configuration files from the 32-bit server to the same directories on the 64-bit computer or virtual machine:

Directory	Description
<code>c:\Vontu\Protect\plugins</code> or <code>/opt/Vontu/Protect/plugins</code>	<p>Copy the entire contents of the <code>plugins</code> directory if you use custom plug-ins.</p> <p>If any plug-ins require resources that reside outside of the <code>plugins</code> directory, copy those resources as well.</p> <p><b>Note:</b> Any plug-ins that use native code must be recompiled for use on the 64-bit detection server computer or virtual machine. Do not copy 32-bit native plugins to the new server.</p>
<code>c:\Vontu\Protect\config</code> or <code>/opt/Vontu/Protect/config</code>	<p>If you manually edited a Symantec Data Loss Prevention properties file (<code>.properties</code> extension) other than <code>jdbc.properties</code>, copy that file to the same location on the 64-bit Enforce Server computer or virtual machine.</p> <p><b>Note:</b> Do not copy the <code>jdbc.properties</code> file to the new server computer or virtual machine. Do not copy any configuration files (<code>.conf</code> extension) to the new computer.</p> <p>Many of the properties in these files define directory and file locations. If you copy a properties file to the 64-bit computer, also edit the file in its new location to ensure that all paths are valid. For example, if you installed the 32-bit Enforce Server on the <code>c:\</code> drive and the 64-bit server on the <code>d:\</code> drive, edit any copied properties files to specify <code>d:\</code> as the root drive.</p>
<code>c:\Vontu\Protect\scan\incremental_index</code> or <code>/var/Vontu/scan/incremental_index</code>	<p>If you configured Network Discover incremental scans, copy the entire <code>incremental_index</code> directory to the 64-bit Enforce Server installation to preserve the index data.</p>

Directory	Description
c:\Vontu\Protect\lib\jdbc or /opt/Vontu/Protect/lib/jdbc	If you added a JDBC driver to the 32-bit detection server, copy the driver to the 64-bit detection server computer or add a 64-bit version of the driver to the 64-bit server.

---

**Note:** On Linux systems, ensure that you preserve the same file permissions and ownership attributes when copying files between systems.

---

- 4 Import any custom certificates that are necessary to communicate with the Enforce Server and any other network component. For example, you may need to reimport MTA certificates on a Network Prevent (Email) server to support TLS communication.  
 See “Configuring certificates for secure communication” in the *Symantec Data Loss Prevention Installation Guide* for your platform.  
 See “Configuring keys and certificates for TLS” in the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)*.
- 5 Start the 64-bit detection server if it is not already running.  
 See “[About starting and stopping services on Windows](#)” on page 70.  
 See “[Starting and stopping services on Linux](#)” on page 73.
- 6 Log in to the Enforce Server administration console for the deployment.
- 7 Select **System > Servers > Overview**.
- 8 Click the name of the 32-bit detection server that you are migrating.
- 9 Click **Configure**.
- 10 Edit the **Host** and **Port** fields to point to the new 64-bit server computer or virtual machine.
- 11 Click **Save**.
- 12 Click **Done**.
- 13 Shut down the 32-bit detection server that you migrated.  
 See “[About starting and stopping services on Windows](#)” on page 70.  
 See “[Starting and stopping services on Linux](#)” on page 73.



# 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](#)
- [Advanced agent settings](#)

## 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 135.

See [“About the Enforce Server administration console”](#) on page 46.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Adding a detection server”](#) on page 166.

See [“Removing a server”](#) on page 167.

See [“Server controls”](#) on page 151.

See [“Server configuration—basic”](#) on page 152.

## 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 172.

The individual processes and the servers on which they run are as follows:

- Monitor Controller (Enforce Server) controls detection server.
- File Reader (all detection servers) detects the incidents.
- Incident Writer (all detection servers, unless they are part of a single-tier installation) uploads the incidents to the Enforce Server.

- Packet Capture (Network Monitor) captures network streams.
- Request Processor (Network Prevent (Email)) processes the SMTP requests.
- Endpoint Server (Endpoint Server) interacts with Symantec DLP Agents.

**To enable Advanced Process Control**

- 1 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**.

See “[Server configuration—basic](#)” on page 152.

Consult Symantec Data Loss Prevention online Help for more information about working with System Settings.

## 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 172.

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 10-1** Server status values

Icon	Status
	Starting - In the process of starting.
	Running - Running without errors.
	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.

**Table 10-1** Server status values (*continued*)

Icon	Status
	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 45.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“System events reports”](#) on page 104.

See [“Server event detail”](#) on page 108.

## 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

- 1 Go to the **Overview** screen (**System > Servers > Overview**).
- 2 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 165.  
See Symantec Data Loss Prevention online Help for information about advanced server configuration.
- 3 Click **Configure** or **Server Settings** to display a configuration screen for that type of server.
  - 4 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 151.

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 installations a **Same as Enforce** option is available. If the detection server is installed on the same host as the Endpoint Server, select this option to automatically populate the Host field with the local IP address (127.0.0.1).

The remaining portions of a **Configure Server** screen vary according to the type of server.

See “[Network Monitor Server—basic configuration](#)” on page 154.

See “[Network Discover Server and Network Protect—basic configuration](#)” on page 162.

See “[Network Prevent \(Email\) Server—basic configuration](#)” on page 156.

See “[Network Prevent \(Web\) Server—basic configuration](#)” on page 159.

See “[Endpoint Server—basic configuration](#)” on page 163.

See “[Classification Server—basic configuration](#)” on page 164.

See “[Server Detail screen](#)” on page 172.

## 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 152.
- **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
<b>Source Folder Override</b>	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.

Field	Description
<b>Archive Folder</b>	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.
<b>Network Interfaces</b>	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 <i>Symantec Data Loss Prevention Installation Guide</i> for more information about NICs.

See “[Implementing Network Monitor](#)” on page 803.

The **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

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 45.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

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 174.

See the Symantec Data Loss Prevention online Help for information about advanced server settings.

## Network Prevent (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 (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 152.

Use the **Inline SMTP** tab to configure different Network Prevent (Email) Server features:

Field	Description
<b>Trial Mode</b>	<p>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.</p>
<b>Keystore Password</b>	<p>If you use TLS authentication in a forwarding mode configuration, enter the correct password for the keystore file.</p>
<b>Confirm keystore Password</b>	<p>Re-enter the keystore file password.</p>
<b>Next Hop Configuration</b>	<p>Select <b>Reflect</b> to operate Network Prevent (Email) Server in reflecting mode. Select <b>Forward</b> to operate in forwarding mode.</p> <p><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.</p>
<b>Enable MX Lookup</b>	<p>This option applies only to forwarding mode configurations.</p> <p>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 (Email) Server uses the returned MX records to select the address of the next hop mail server.</p> <p>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:</p> <p><code>companyname.com</code></p> <p>Network Prevent (Email) Server performs MX record queries for the domain names that you specify.</p> <p><b>Note:</b> You must include at least one valid entry in the <b>Enter Domains</b> text box to successfully configure forwarding mode behavior.</p>

Field	Description
<b>Disable MX Lookup</b>	<p>This field applies only to forwarding mode configurations.</p> <p>Select <b>Disable MX Lookup</b> if you want to specify the exact hostname or IP address of one or more next-hop MTAs. Network Prevent (Email) Server uses the hostnames or addresses that you specify and does not perform an MX record lookup.</p> <p>If you select <b>Disable MX Lookup</b>, also add one or more hostnames or IP addresses for next-hop MTAs in the <b>Enter Hostnames</b> text box. You can specify multiple entries by placing each entry on a separate line. For example:</p> <pre>smtp1.companyname.com smtp2.companyname.com smtp3.companyname.com</pre> <p>Network Prevent (Email) Server always tries to use the first MTA that you specify in the list. If that MTA is not available, Network Prevent (Email) Server tries the next available entry in the list.</p> <p><b>Note:</b> You must include at least one valid entry in the <b>Enter Hostnames</b> text box to successfully configure forwarding mode behavior.</p>

See the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)* for additional information about configuring Network Prevent (Email) Server options.

See [“About Symantec Data Loss Prevention administration”](#) on page 45.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

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 174.

See the Symantec Data Loss Prevention online Help for information about advanced server settings.

## Network Prevent (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 (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 152.
- **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
<b>Ignore Requests Smaller Than</b>	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.
<b>Ignore Requests without Attachments</b>	Check this box to inspect only those HTTP requests that contain attachments.

Field	Description
<b>Ignore Requests to Hosts or Domains</b>	Enter the host names or domains whose requests should be filtered out (ignored). Enter one host or domain name per line.
<b>Ignore Requests from User Agents</b>	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
<b>Ignore Responses Smaller Than</b>	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.
<b>Inspect Content Type</b>	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 <b>application/wordperfect5.1</b> .
<b>Ignore Responses from Hosts or Domains</b>	Enter the host names or domains whose responses are to be ignored. Enter one host or domain name per line.

Field	Description
<b>Ignore Responses to User Agents</b>	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 (Web) Server:

Field	Description
<b>TCP Port</b>	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.
<b>Maximum Number of Requests</b>	Enter the maximum number of simultaneous ICAP connections from the HTTP proxy that are allowed. The default is 25.
<b>Maximum Number of Responses</b>	Enter the maximum number of simultaneous ICAP response connections from the HTTP proxy or proxies that are allowed. The default is 25.
<b>Connection Backlog</b>	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 \(Web\) Server”](#) on page 829.

See [“About Symantec Data Loss Prevention administration”](#) on page 45.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

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 174.

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 848.

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 152.
- **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 server.

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 45.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

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 174.

## 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 166.

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 152.
- **Agent.** This section is for configuring the Endpoint Server to a specific endpoint configuration.  
See [“Adding agent configurations”](#) on page 1082.

**Agent Listener.** Use this section to configure the Endpoint Server to listen for connections from Symantec DLP Agents:

Field	Description
<b>Bind address</b>	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.
<b>Port</b>	Enter the port over which the Endpoint Server listens for communications from the Symantec DLP Agents.

**Agent Configuration.** Use this section to specify which agent configuration module you want to associate with the new Endpoint Server.

Field	Description
Agent Configuration	Use the drop-down menu to select the agent configuration module that you want. If only one module has been defined, Endpoint Servers are automatically associated with the agent configuration.

See “[About agent configurations](#)” on page 1081.

## Classification 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. 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 152.
- **Classification** section. This section specifies 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:

<b>Maximum number of sessions</b>	Enter the maximum number of concurrent sessions that the Classification Server will 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 <i>Symantec Enterprise Vault Data Classification Services Implementation Guide</i> for more information.
<b>Session Timeout (in milliseconds)</b>	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 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.

---

## 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

- 1 Go to **System > Servers > Overview** and click on the name of the detection server.  
That server's **Server Detail** screen appears.
- 2 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 174.
- 3 With the guidance of Symantec Support, modify the appropriate setting(s).
- 4 Click **Save**.  
Changes to settings on this screen normally do not take effect until you restart the server.

See [“Server configuration—basic”](#) on page 152.

## 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 Protect Server, which inspects stored data for policy violations (Network Discover).
- Network Prevent (Email) Server, which prohibits SMTP violations.
- Network Prevent (Web) Server, which prohibits ICAP proxy server violations such as FTP, HTTP, and HTTPS.
- Endpoint Server, which controls Symantec DLP Agents that monitor endpoint computers.
- Classification Server, which analyzes email messages that are 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.

### To add a detection server

- 1 Go to the **System Overview** screen (**System > Servers > Overview**).  
See [“About the System Overview screen”](#) on page 169.
- 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 154.  
See [“Network Prevent \(Email\) Server—basic configuration”](#) on page 156.  
See [“Network Prevent \(Web\) Server—basic configuration”](#) on page 159.  
See [“Network Discover Server and Network Protect—basic configuration”](#) on page 162.  
See [“Endpoint Server—basic configuration”](#) on page 163.  
See [“Classification Server—basic configuration”](#) on page 164.

- 5 To return to the **System Overview** screen, click **Done**.  
Your new server is displayed in the **Servers** list with a status of **Unknown**.
- 6 Click on the server to display its **Server Detail** screen.  
See “[Server Detail screen](#)” on page 172.
- 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 is **Running**.
- 9 If necessary, click **Server Settings** on the server's **Server Detail** screen to perform advanced server configuration.  
See “[Advanced server settings](#)” on page 174.  
See Symantec Data Loss Prevention online Help for information about advanced server configuration.  
See “[Server configuration—basic](#)” on page 152.

## 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**

- 1 Go to **System > Overview**.  
See “[About the System Overview screen](#)” on page 169.
- 2 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 151.
- 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.

**Table 10-2** Importing an SSL certificate to Enforce or Discover

Step	Description
1	Copy the certificate file you want to import to the Enforce Server or Discover Server computer.
2	Change directory to <code>c:\Vontu\jre\bin</code> on the Enforce Server or Discover Server computer.
3	Execute the <code>keytool</code> utility with the <code>-importcert</code> option to import the public key certificate to the Enforce Server or Discover Server keystore:  <pre>keytool -importcert -alias <i>new_endpointgroup_alias</i> -keystore..\lib\cacerts -file <i>my-domaincontroler.crt</i></pre> In this example command, <i>new_endpointgroup_alias</i> is a new alias to assign to the imported certificate and <i>my-domaincontroler.crt</i> is the path to your certificate.

**Table 10-2** Importing an SSL certificate to Enforce or Discover (*continued*)

Step	Description
4	<p>When you are prompted, enter the password for the keystore.</p> <p>By default, the password is <b>changeit</b>. If you want you can change the password when prompted.</p> <p>To change the password, use: <code>keytool -storepassword -keystore..\lib\security\cacerts</code></p>
5	Answer <b>Yes</b> when you are asked if you trust this certificate.
6	Restart the Enforce Server or Discover Server.

See “[Creating and managing directory server connections](#)” on page 513.

## About the System Overview screen

The **System Overview** screen is reached by **System > Servers > Overview**. This screen provides a quick 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 166.
- The **Upgrade button** is for upgrading Symantec Data Loss Prevention to a newer version. See “[About system upgrades](#)” on page 136. 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 170.
- 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 172.
- 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 152.

See [“About Symantec Data Loss Prevention administration”](#) on page 45.

## 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 10-3** Server statuses

Icon	Status	Description
	Starting	The server is starting up.
	Running	The server is running normally without errors.
	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 <a href="#">“Enabling Advanced Process Control”</a> on page 150.
	Stopping	The server is in the process of stopping Symantec Data Loss Prevention services.  See <a href="#">“About Enforce Server services”</a> on page 69.
	Stopped	All Symantec Data Loss Prevention processes are stopped.
	Unknown	The server is experiencing one of the following errors: <ul style="list-style-type: none"> <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 10-4** 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.
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.

**To see details about a server**

- ◆ Click on any server name to see additional details regarding that server. See “[Server Detail screen](#)” on page 172.

**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 167.

## Recent error and warning events list

The **Recent Error and Warning Events** section of the **System Overview** screen is reached by **System > 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.

**Table 10-5** Recent error and warning events information

Column name	Description
Type	  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.

- 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 169.

See [“System events reports”](#) on page 104.

See [“Server event detail”](#) on page 108.

## Server Detail screen

The **Server Detail** 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 169.

The **Server Detail** screen is divided into sections. The sections listed below are displayed for all server types. The system displays sections based on the type of detection server.

**Table 10-6** Server Detail screen display information

Server Detail display sections	Description
General	<p>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.</p> <p>See <a href="#">“Server controls”</a> on page 151.</p>
Configuration	<p>The <b>Configuration</b> section displays the Channels, Policy Groups, Agent Configuration, and Configuration Status for the detection server.</p>
Agent Summary	<p>The <b>Agent Summary</b> section displays a summary of all agents assigned to the Endpoint Server.</p> <p>Click <b>All Agents</b> to go to the <b>System &gt; Agents &gt; Overview</b> screen and view the details for each agent.</p> <p><b>Note:</b> The system only displays the <b>Agent Summary</b> section for an Endpoint Server.</p>
Recent Error and Warning Events	<p>The <b>Recent Error and Warning Events</b> section displays the five most recent Warning or Severe events that have occurred on this server.</p> <p>Click on an event to show event details. Click <b>show all</b> to display all error and warning events.</p> <p>See <a href="#">“About system events”</a> on page 103.</p>
All Recent Events	<p>The <b>All Recent Events</b> section displays all events of all severities that have occurred on this server during the past 24 hours.</p> <p>Click on an event to show event details. Click <b>show all</b> to display all detection server events.</p>

**Table 10-6** Server Detail screen display information (*continued*)

Server Detail display sections	Description
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 <a href="#">“About Data Profiles”</a> on page 316.

See [“About the System Overview screen”](#) on page 169.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

See [“System events reports”](#) on page 104.

See [“Server event detail”](#) on page 108.

## 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. It is recommended that you check with 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.

There are no advanced settings on the Enforce Server that can be modified from its server detail screen.

**Table 10-7** Detection server advanced settings

Setting	Default	Description
BoxMonitor.Channels	varies	<p>The values are case sensitive and comma-separated if multiple.</p> <p>Although any mix of them can be configured, the following are the officially supported configurations:</p> <ul style="list-style-type: none"> <li>■ Network Monitor Server: <b>Packet Capture, Copy Rule</b></li> <li>■ Discover Server: <b>Discover</b></li> <li>■ Endpoint Server: <b>Endpoint</b></li> <li>■ Network Prevent (Email): <b>Inline SMTP</b></li> <li>■ Network Prevent (Web): <b>ICAP</b></li> <li>■ Classification Server: <b>Classification</b></li> </ul>
BoxMonitor.DiskUsageError	<b>90</b>	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	<b>80</b>	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 80, then the detection server generates a warning system event when the C drive usage is above 80%
BoxMonitor.EndpointServer	<b>on</b>	Enables the Endpoint Server.
BoxMonitor.EndpointServerMemory		Any combination of JVM memory flags can be used. For example: <b>-Xrs -Xms300M -Xmx1024M</b>
BoxMonitor.FileReader	<b>on</b>	If off, the BoxMonitor cannot start the FileReader, although it can still be started manually.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
BoxMonitor.FileReaderMemory		FileReader JVM command line arguments. For example: <b>-Xrs -Xms1200M -Xmx1200M</b>
BoxMonitor.HeartbeatGapBeforeRestart	<b>960000</b>	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	<b>on</b>	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	<b>5000</b>	
BoxMonitor.MaxRestartCount	<b>3</b>	
BoxMonitor.MaxRestartCountDuringStartup	<b>5</b>	The maximum times that the Monitor server will attempt to restart on its own.
BoxMonitor.PacketCapture	<b>on</b>	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: <b>-Xrs</b>
BoxMonitor.ProcessLaunchTimeout	<b>30000</b>	The time interval (in milliseconds) for a monitor process (e.g. FileReader) to start.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
BoxMonitor.ProcessShutdownTimeout	<b>45000</b>	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.
BoxMonitor.RequestProcessor	<b>on</b>	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: <b>-Xrs -Xms300M -Xmx1300M</b>
BoxMonitor.RmiConnectionTimeout	<b>15000</b>	The time interval (in milliseconds) allowed to establish connection to the RMI object.
BoxMonitor.RmiRegistryPort	<b>37329</b>	The TCP port on which the BoxMonitor starts the RMI registry.
BoxMonitor.StatisticsUpdatePeriod	<b>10000</b>	The monitor statistics are updated after this time interval (in milliseconds).
Classification.BindAddress	<b>0.0.0.0</b>	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	<b>120M</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
Classification.SessionReapInterval	<b>20000</b>	The time interval (in milliseconds) after which the Classification Server purges stale sessions.
Classification.WebserviceLogRetentionDays	<b>7</b>	The number of days to retain the Classification Server web service request log. These log files are stored in the c:\Vontu\Protect\logs\jetty (Windows) or /var/log/Vontu/logs/jetty (Linux) ..
ContentExtraction.EnableMetaData	<b>off</b>	Allows detection on file metadata. For example, in MS Word the metadata fields Title, Subject, Author, or Keywords. Enabling this option can cause false positives. The default is set to disallow.
ContentExtraction.LongContentSize	<b>1M</b>	If the message component exceeds this size (in bytes) then the ContentExtraction.LongTimeout is used instead of ContentExtraction.ShortTimeout.
ContentExtraction.LongTimeout	Varies	The default value for this setting varies depending on detection server type ( <b>60,000</b> or <b>120,000</b> ).  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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
ContentExtraction.MarkupAsText	<b>off</b>	Bypasses Content Extraction for files that are determined to be XML or HTML. This should be used in cases such as web 2.0 pages containing data in the header block or script blocks. Default is off.
ContentExtraction.MaxContentSize	<b>30M</b>	The maximum size (in MB) of the document that can be processed by the ContentExtractor.
ContentExtraction.RunawayTimeout	<b>300,000</b>	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.
ContentExtraction.ShortTimeout	<b>30,000</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
ContentExtraction.TrackedChanges	<b>off</b>	<p>Allows detection of content that has changed over time (Track Changes content) in Microsoft Office documents.</p> <p><b>Note:</b> Using the foregoing option might reduce the accuracy rate for IDM and data identifiers. The default is set to off (disallow).</p> <p>To index content that has changed over time, set ContentExtraction.TrackedChanges=on in the C:\Vontu\Protect\config\Indexer.properties file. The default and recommended setting is ContentExtraction.TrackedChanges=off.</p>
DDM.MaxBinMatchSize	<b>300,000,000</b>	<p>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:</p> <ul style="list-style-type: none"> <li>■ 1 - This setting must be exactly identical to the max_bin_match_size setting on the Enforce Server in the indexer.properties file.</li> <li>■ 2 - This setting must be smaller or equal to the FileReader.FileMaxSize value.</li> <li>■ 3 - This setting must be smaller or equal to the ContentExtraction.MaxContentSize value on the Enforce Server in the indexer.properties file.</li> </ul> <p><b>Note:</b> Changing 1) and/or 3) requires re-indexing all IDM files.</p>

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
DDM.UseJavaMD5	<b>false</b>	If true, use the third-party library to generate MD5 hashes. If false, use the Java default MD5 library. In general, this setting should not be changed.
Detection.EncodingGuessingDefaultEncoding	<b>ISO-8859-1</b>	Specifies the backup encoding assumed for a byte stream.
Detection.EncodingGuessingEnabled	<b>on</b>	Designates whether the encoding of unknown byte streams should be guessed.
Detection.EncodingGuessingMinimumConfidence	<b>50</b>	Specifies the confidence level required for guessing the encoding of unknown byte streams.
DI.MaxViolations	<b>100</b>	Specifies the maximum number of violations allowed with data identifiers.
Discover.CountAllFilteredItems	<b>false</b>	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	<b>false</b>	Specifies whether to follow redirects.
Discover.Exchange.ScanHiddenItems	<b>false</b>	Scan hidden items in Exchange repositories, when set to true.
Discover.IgnorePstMessageClasses		The default setting is: <del>Empty</del> 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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
Discover.IncludePstMessageClasses	<b>IPM.Note</b>	<p>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.</p> <p>When both the include setting and the ignore setting are defined, Discover.IncludePstMessageClasses takes precedence.</p>
Discover.PollInterval	<b>10000</b>	Specifies the time interval (in milliseconds) at which Enforce retrieves data from the Discover monitor while scanning.
Discover.Sharepoint.FetchACL	<b>true</b>	Turns off ACL fetching for integrated SharePoint scans. The default value is true (on).
Discover.ValidateSSLCertificates	<b>false</b>	<p>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 <code>keytool</code> utility.</p> <p>See <a href="#">“Importing SSL certificates to Enforce or Discover servers”</a> on page 168.</p>

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
EDM.MatchCountVariant	3	<p>Specifies how matches are counted.</p> <ul style="list-style-type: none"> <li>■ 1 - counts the number of matched database rows regardless of use of the same tokens across several matches</li> <li>■ 2 - eliminates matches that consist of identical sets of tokens</li> <li>■ 3 - eliminates matches that consist of a subset of tokens from some other match (the default)</li> </ul> <p>See <a href="#">“About configuring exact data match counting”</a> on page 371.</p>
EDM.MaximumNumberOfMatchesToReturn	100	<p>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.</p>
EDM.RunProximityLogic	true	<p>If true, runs the token proximity check. The free-form (a.k.a. simple) text proximity is defined by EDM.SimpleTextProximityRadius setting. The tabular text proximity is defined by belonging to the same table row.</p>
EDM.SimpleTextProximityRadius	35	<p>Number of tokens to the left and to the right of the current token that are evaluated together when the proximity check is enabled.</p>
EDM.VerifyJohnJohnCases	true	<p>Specifies whether to consider matches where more than one database column has the same value. For example, the first name is John and the last name is John. This verification incurs a slight performance penalty.</p>

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
EndpointMessageStatistics.MaxFileDetectionCount	<b>100</b>	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	<b>1800</b>	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	<b>2000</b>	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	<b>3</b>	The maximum list of hosts displayed from where valid files, folders, and messages come. When a system event for EndpointMessageStatistics.MaxFileDetectionCount, EndpointMessageStatistics.MaxFolderDetectionCount, or EndpointMessageStatistics.MaxMessageCount 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	<b>10000</b>	The interval of time in milliseconds the aggregator will accumulate scan statuses before sending them to the MonitorController as a batch.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
EndpointServer.EndpointSystemEventQueueSize	<b>20000</b>	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.MaxPercentageMemToStoreEndpointFiles	<b>60</b>	The maximum amount (in percentage) of memory to use to store shadow cache files.
EndpointServer.MaxTimeToKeepEndpointFilesOpen	<b>20000</b>	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	<b>1000</b>	The maximum time (in milliseconds) that the agent will wait to connect to the server.
EndpointServer.NoOfRecievers	<b>15</b>	The number of endpoint shadow cache file receivers.
EndpointServer.NoOfWriters	<b>10</b>	The number of endpoint shadow cache file writers.
FileReader.MaxFileSize	<b>30M</b>	The maximum size (in MB) of a message to be processed. Larger messages are truncated to this size.
FileReader.MaxFileSystemCrawlerMemory	<b>30M</b>	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	<b>15</b>	The time that a child process can have data but not have read anything before it stops sending heartbeats.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
FileReader.ScheduledInterval	<b>1000</b>	The time interval (in milliseconds) between drop folder checks by the filereader. This affects Copy Rule, Packet Capture, and File System channels only.
Icap.AllowHosts	<b>any</b>	The default value of "any" permits all systems to make a connection to the Network Prevent Server (Web) 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 or FQDNs by commas.
Icap.AllowStreaming	<b>false</b>	If true, ICAP output is streamed to the proxy directly without buffering the ICAP request first. NetApp NetCache 6.0 does not support such streaming.
Icap.BindAddress	<b>0.0.0.0</b>	IP address to which a Network Prevent Server (Web) 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	<b>3K</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
Icap.DisableHealthCheck	<b>false</b>	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.
Icap.EnableTrace	<b>false</b>	If set to true, protocol debug tracing is enabled once a folder is specified using the Icap.TraceFolder setting.
Icap.LoadBalanceFactor	<b>1</b>	The number of web proxy servers that a Network Prevent (Web) server 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.SpoolFolder		This value is needed for ICAP Spools. This setting must be set to the correct drive letter when updating from Vontu DLP 5.0 U3 to 6.0 GA; otherwise, the FileReader will not start.
Icap.TraceFolder		The fully qualified name of the folder or directory where protocol debug trace data is stored when the Icap.EnableTrace setting is true. By default, the value for this setting is left blank.
IncidentDetection.IncidentLimitResetTime	<b>86400000</b>	Specifies the time frame (in milliseconds) used by the IncidentDetection.MaxIncidentsPerPolicy setting. The default setting 86400000 equals one day.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
IncidentDetection.MaxContentLength	<b>2000000</b>	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	<b>10000</b>	Defines the maximum number of incidents detected by a specific policy on a particular monitor within the time-frame specified in the IncidentDetection.IncidentTimeLimitResetTime. The default is 10,000 incidents per policy per time limit.
IncidentDetection.MessageWaitSevere	<b>240</b>	The number of minutes to wait before sending a severe system event about message wait times.
IncidentDetection.MessageWaitWarning	<b>60</b>	The number of minutes to wait before sending a warning system event about message wait times.
IncidentDetection.MinNormalizedSize	<b>30</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
IncidentDetection.patternConditionMaxViolations	<b>100</b>	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	<b>400M</b>	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.
IncidentDetection.TrialMode	<b>false</b>	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	<b>1000</b>	The number of incidents that collect in the log before an information level message about the number of messages is generated.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
IncidentWriter.BacklogSevere	<b>10000</b>	The number of incidents that collect in the log before a severe level message about the number of messages is generated.
IncidentWriter.BacklogWarning	<b>3000</b>	The number of incidents that collect in the log before a warning level message about the number of messages is generated.
IncidentWriter.ResolveIncidentDNSNames	<b>false</b>	If true, only recipient host names are resolved from IP.
IncidentWriter.ShouldEncryptContent	<b>true</b>	If true, the monitor will encrypt the body of every message, message component and cracked component before writing to disk or sending to Enforce.
L7.cleanHttpBody	<b>true</b>	If true, the HTML entity references are replaced with spaces.
L7.DefaultBATV	<b>Standard</b>	This setting determines the tagging scheme that Network Prevent (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 <a href="http://tools.ietf.org/html/draft-levine-mass-batv-02">http://tools.ietf.org/html/draft-levine-mass-batv-02</a> ). Change this setting to “Ironport” to enable compatibility with the IronPort proxy’s implementation of BATV tagging.
L7.DefaultUrlEncodedCharset	<b>UTF-8</b>	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	<b>true</b>	If true, the Monitor ignores duplicate messages based on the messageID.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
L7.ExtractBATV	<b>true</b>	If true (the default), Network Prevent (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 (Email) does not interpret BATV tags, and a message that contains BATV tags may generate an incident that has an unreadable sender address.  See <a href="http://tools.ietf.org/html/draft-levine-mass-batv-02">http://tools.ietf.org/html/draft-levine-mass-batv-02</a> for more information about BATV.
L7.httpClientIdHeader		The sender identifier header name. The default setting is <b>X-Forwarded-For</b> .
L7.MAX_NUM_HTTP_HEADERS	<b>30</b>	If any HTTP message that contains more than the specified header lines, it is discarded.
L7.maxWordLength	<b>30</b>	The maximum word length (in characters) allowed in UTCP string extraction.
L7.messageIDCacheCleanupInterval	<b>600000</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
L7.minSizeOfGetUrl	<b>100</b>	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: <a href="http://www.symantec.com/index.jsp">http://www.symantec.com/index.jsp</a> . The reason is that the URL contains only 33 characters which is less than the 100 minimum. <b>Note:</b> 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	<b>true</b>	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.AllowCommasWithOtherSeparatorInTabular	<b>true</b>	
Lexer.IncludeLinesWithOnlyWordsInTabular	<b>false</b>	If true, words-only lines are recognized as tabular data.
Lexer.IncludePostalCodeInMultiWord	<b>true</b>	If true, postal code is included in multi-word columns of tabular text.
Lexer.IncludePunctuationInWords	<b>true</b>	If true, punctuation characters are considered as part of a word.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
Lexer.MaximumNumberOfTokens	<b>30000</b>	Maximum number of tokens (including separators) extracted from each message component for detection. Applicable to all detection technologies where tokenization is required, e.g. System patterns, EDM, DGM. Increasing this value may cause the detection to run out of memory and restart. Default is 30,000.
Lexer.MultiWordRecognition	<b>true</b>	If true, multi-word columns are recognized in tabular data.
Lexer.StopwordLanguages	<b>en</b>	Enables the elimination of stop words for the specified languages. The default is English.
Lexer.Validate	<b>true</b>	If true, performs system pattern-specific validation.
MessageChain.ArchiveTimedOutStreams	<b>false</b>	Specifies whether messages should be archived to the temp folder
MessageChain.CacheSize	<b>8</b>	Limits the number of messages that can be queued in the message chains.
MessageChain.ContentDumpEnabled	<b>false</b>	
MessageChain.MaximumComponentTime	varies	This setting is either <b>60000</b> or <b>360,000</b> depending on detection server type. The time interval (in milliseconds) allowed before any chain component is restarted.
MessageChain.MaximumFailureTime	<b>360000</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
MessageChain.MaximumMessageTime	varies	This setting varies between is either <b>600,000</b> or <b>1,800,000</b> depending on detection server type.  The maximum time interval (in milliseconds) that a message can remain in a message chain.
MessageChain.MemoryThrottlerReservedBytes	<b>200,000,000</b>	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 zero.
MessageChain.MinimumFailureTime	<b>30000</b>	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.
MessageChain.NumChains	varies	This number varies depending on detection server type. It is either <b>4</b> or <b>8</b> .  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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
MessageChain.StopProcessingWhenMemoryLowerThan	<b>200M</b>	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	<b>true</b>	If true, discards HTTP GET streams.
PacketCapture.DOES_DISCARD_TRIGGER_STREAM_DUMP	<b>false</b>	If true, a list of tcpstreams is dumped to an output file in the log directory the first time a discard message is received.
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

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
PacketCapture.Filter		The default setting is <b>tcp    ip proto 47    (vlan &amp;&amp; (tcp    ip proto 47))</b> .  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	<b>/dummy.dmp</b>	The full path and name of the input file.
PacketCapture.IS_ARCHIVING_PACKETS	<b>false</b>	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	<b>false</b>	To enable packet-capture using an Endace card, set this value to true.
PacketCapture.IS_FTP_RETR_ENABLED	<b>false</b>	If true, FTP GETS and FTP PUTS are processed. If false, only process FTP PUTS are processed.
PacketCapture.IS_INPUT_SOURCE_FILE	<b>false</b>	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.KERNEL_BUFFER_SIZE_I686	<b>64M</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
PacketCapture.KERNEL_BUFFER_SIZE_Win32	<b>16M</b>	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	<b>64M</b>	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.
PacketCapture.KERNEL_BUFFER_SIZE_X86_64	<b>64M</b>	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	<b>30000</b>	After the specified number of file streams are processed a new directory is created.
PacketCapture.MBYTES_LEFT_TO_DISABLE_CAPTURE	<b>1000</b>	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	<b>1500</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
PacketCapture.NO_TRAFFIC_ALERT_PERIOD	<b>86,400</b>	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	<b>600000</b>	The number of standard sized preallocated packet buffers used to buffer and sort incoming traffic.
PacketCapture.NUMBER_JUMBO_POOL_PACKETS	<b>1</b>	The number of large sized preallocated packet buffers that are used to buffer and sort incoming traffic.
PacketCapture.NUMBER_SMALL_POOL_PACKETS	<b>200000</b>	The number of small sized preallocated packet buffers that are used to buffer and sort incoming traffic.
PacketCapture.RING_CAPTURE_LENGTH	<b>1518</b>	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.
PacketCapture.RING_DEVICE_MEM	<b>67108864</b>	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	<b>1540</b>	The size of standard-sized buffer pool packets.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
PacketCapture.SIZE_JUMBO_POOL_PACKETS	<b>10000</b>	The size of jumbo-sized buffer pool packets.
PacketCapture.SIZE_SMALL_POOL_PACKETS	<b>150</b>	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	<b>5000</b>	The time (in milliseconds) between each count (StreamManager's write timeout)
ProfileIndex.CheckAvailableRAM	<b>true</b>	Specifies whether or not the amount of available RAM should be compared with a profile size before loading an EDM or IDM profile. Set to false for single tier installations otherwise EDM file may fail to index.
ProfileIndex.MaximumInProgressIndexSize	<b>100M</b>	Specifies an upper limit for the maximum In Process index size. Profiles that exceed this size are loaded out of process by RMI.
ProfileIndex.MinimumMemoryReserve	<b>200M</b>	Specifies the memory reserved for out-of-process EDM and/or IDM algorithm execution. It's used to calculate the JVM heap size as $index\_size + MinimumMemoryReserve$ . Supported by IDM since v7 and by EDM since v8.
ProfileIndex.ProcessTimeout	<b>10000</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
RequestProcessor.AddDefaultHeader	<b>true</b>	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.
RequestProcessor.AllowExtensions		The default setting is: <b>8BITMIME VRFY DSN HELP PIPELINING SIZE ENHANCEDSTATUSCODES STARTTLS</b>  This setting lists the SMTP protocol extensions that Network Prevent (Email) can use when it communicates with other MTAs.
RequestProcessor.AllowHosts	<b>any</b>	The default value of any permits all systems to make connections to the Network Prevent Server (Email) 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	<b>false</b>	The default value ensures that MTAs must authenticate with Network Prevent (Email) for TLS communication.
RequestProcessor.Backlog	<b>12</b>	The backlog that the request processor specifies for the server socket listener.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
Requestprocessor.BindAddress	<b>0.0.0.0</b>	IP address to which a Network Prevent Server (Email) 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.
Requestprocessor.DefaultCommandTimeout	<b>300</b>	Specifies the number of seconds the Network Prevent Server (Email) 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		The default setting is: <b>X-C Filter-Loop: Reflected.</b>  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	<b>600</b>	Specifies the number of seconds the Network Prevent Server (Email) 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	<b>20000</b>	The timeout value to use when forwarding to an MTA.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
RequestProcessor.KeyManagementAlgorithm	<b>SunX509</b>	The key management algorithm used in TLS communication.
RequestProcessor.MaxLineSize	<b>1048576</b>	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.
RequestProcessor.Mode	<b>ESMTP</b>	Specifies the protocol mode to use (SMTP or ESMTP).
RequestProcessor.MTAResubmitPort	<b>10026</b>	This is the port number used by the request processor on the MTA to resend the SMTP message.
RequestProcessor.NumberOfDNSAttempts	<b>4</b>	The maximum number of DNS queries that Network Prevent (Email) performs when it attempts to obtain mail exchange (MX) records for a domain. Network Prevent (Email) uses this setting only if you have enabled MX record lookups.
RequestProcessor.RPLTimeout	<b>360000</b>	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	<b>10025</b>	The port number to be used by the SMTP monitor to listen for incoming connections from MTA.
RequestProcessor.TagHighestSeverity	<b>false</b>	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.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
RequestProcessor.TagPolicyCount.	<b>false</b>	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.
RequestProcessor.TagScore	<b>false</b>	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	<b>PKIX</b>	The trust management algorithm that Network Prevent (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	<b>12355</b>	The local TCP port that FileReader will use to listen for connections from RequestProcessor on a Network Prevent server.
SocketCommunication.BufferSize	<b>8K</b>	The size of the buffer that Network Prevent (Web) uses to process ICAP requests. Increase the default value only if you need to process ICAP requests that are greater than 8K.

**Table 10-7** Detection server advanced settings (*continued*)

Setting	Default	Description
UnicodeNormalizer.AsianCharRanges	<b>default</b>	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
UnicodeNormalizer.Enabled	<b>on</b>	Can be used to disable Unicode normalization. Enter <b>off</b> to disable.
UnicodeNormalizer.NewlineEliminationEnabled	<b>on</b>	Can be used to disable newline elimination for Asian languages. Enter <b>off</b> to disable.

See [“About Symantec Data Loss Prevention administration”](#) on page 45.

See [“Advanced agent settings”](#) on page 204.

See [“About the System Overview screen”](#) on page 169.

See [“Server Detail screen”](#) on page 172.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

## 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 server detail page, please contact Symantec Support before making any changes.

[Table 10-8](#) provides a list of server settings, along with the default value and description of each setting.

**Table 10-8** 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.
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.
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.
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 be simultaneously connected to the agent.
ApplicationConnector.TEMPORARY_DIRECTORY.str	%TMP%	The temporary location where application hooks store obfuscated content .

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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 Symantec DLP Agent runs on the endpoint computer.
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. Setting this value to 0 disables 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.int	1	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.DAR_THREAD_PRIORITY.str	BELOW_NORMAL	The priority of the detection thread while it applies policies to text for Endpoint Discover scans.
Detection.FILTER_TIMEOUT.int	420000	The time limit, in milliseconds, for filtering text.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
Detection.LOCAL_DRIVE_KVOOP_PRIORITY.str	BELOW_NORMAL	The priority of the external kvoop process while it extracts text for local drive events.
Detection.LOCAL_DRIVE_THREAD_PRIORITY.str	BELOW_NORMAL	The priority of the detection thread while it applies policies to 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. This setting should be used in cases such as web 2.0 pages containing data in the header block or script blocks.
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_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.NEWLINE_ELIMINATION.str	on	Sets whether newlines are eliminated before detection. The default setting is On.
Detection.RULESRESULTSCACHE_ENABLED.str	on	Rules results caching (RRC) is a way to cache the results of content on a DLP Agent that does not violate a policy.  See <a href="#">“Introduction to policy detection”</a> on page 281.  By default, RRC is set to On. If you do not want to use RRC, set this parameter to Off.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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. The default is set to off.
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.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
Discover.SCAN_ONLY_WHEN_IDLE.int	2	<p>Sets whether the agent performs an Endpoint Discover scan while the endpoint user is idle.</p> <p>If set to 1, the agent only performs Endpoint Discover scanning while the endpoint user is idle.</p> <p>If set to 2, the agent only scans small files while the endpoint computer is active and larger files while the endpoint user is idle. Files taking longer than <code>Discover.SHORT_DETECT_TIME</code> seconds are considered large.</p> <p>If set to 0, the scan runs regardless of user activity.</p>
Discover.SECONDS_UNTIL_IDLE.int	120	<p>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.</p>
Discover.STANDARD_REPORT_INTERVAL.int	10000	<p>The interval of time, in milliseconds, between two Endpoint Discover status reports, while a scan is running.</p>
FileService.MAX_CACHE_SIZE.int	250	<p>The maximum number of recently opened file paths that have been recorded for each endpoint computer process.</p>

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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. Enabled by default. In case this configuration is not found in the database, then this functionality is disabled by default. Set to 0 to enable.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
FileSystem.ENABLE_VEP_FILE_ELIMINATION.int	1	<p>When the setting is enabled, the system does not create the VEP file. Instead it runs detection on the original file and resolves any sharing violations for EDPA.exe and KVOOP.exe, when needed. By default, this setting is disabled. To enable, set to 1.</p> <p><b>Note:</b> Enable this setting if your environment does not contain any of the following:</p> <ul style="list-style-type: none"> <li>■ Data retention policies</li> <li>■ Two-tier detection policies</li> <li>■ Endpoint Discover or Endpoint Prevent encryption software</li> </ul>
FileSystem.NUM_TIMES_TO_OVERWRITE_FILE.int	2	<p>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.</p>
FileSystem.USE_CDDVD_DEFAULT_EXCLUDE_PATHS.int	1	<p>This setting allows user to exclude any file that is opened by a CD/DVD application from the following directories:</p> <ul style="list-style-type: none"> <li>■ Installed directory of the application, for example; if the application is Roxio, then c:\program files\roxio</li> <li>■ System directories; for example, %windir%\system32</li> <li>■ Program files\common files.</li> </ul> <p>It is enabled by default.</p>

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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 Plugin Host can take to start up. The default time is in milliseconds. If the Plugin Host does not start in the specified amount of time, the Plugin Host sends a fail event to the log.
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_HOOKING.int	3	Allows the Symantec DLP Agent to monitor Microsoft Internet Explorer traffic.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
Hooking .USE_LOADLIBRARYW_FROM_IMAGE.int	0	<p>The method to find the LoadLibraryW function address. You can specify a value of either 0 or 1.</p> <p>0 uses the GetProcAddress API to find the library.</p> <p>1 reads the exports table of kernel32.dll to find the library.</p>
IE8_HTTPS.Monitor.int	1	<p>Sets IE8 HTTPS monitoring for Symantec DLP Agent v9.x. IE8 HTTPS monitoring for Symantec DLP Agent v10.0 is automatic. Monitoring is set to on by default. To disable, set to 0.</p>
IncidentHandler.CACHE_SIZE_THRESHOLD.int	30	<p>The percentage of used endpoint database cache space that triggers Endpoint Discover to pause.</p>
IncidentHandler.MAX_BACKOFF.int	3600000	<p>Maximum time, in milliseconds, to wait before it retries to send an incident to the Server if the first attempt fails.</p>
IncidentHandler.MAX_INCIDENT_FILE_SIZE	31457280	<p>Size, in bytes, of the largest file to be sent from the agent for two-tier detection.</p>
IncidentHandler.MAX_TTD_FILE_SIZE	31457280	<p>Size, in bytes, of the largest file to be sent from agent for two-tier detection.</p>
IncidentHandler.MIN_BACKOFF.int	30000	<p>Minimum time, in milliseconds, to wait before the agent re-sends an incident to the Endpoint Server after the first attempt fails.</p>

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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.
Logging.OperationLogMaxFiles.int	30	The maximum number of operation logs 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.
Logging.OperationLogTTL.int	90	The length of time that operational logs are kept in the directory. If the operational log is not accessed or modified in the specified amount of time, the file is deleted.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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.
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.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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 turn on 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 popup notification. This setting applies to File System DIM events only.
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 popup notification. This setting applies to HTTP, FTP & 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.
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 popup notification within the specified time.
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 popup notification. This setting applies to Clipboard, Print, Email, HTTPS events only.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
Quarantine.MAX_QUEUE_SIZE.int	100	The maximum number of quarantine requests that can be in queue at any one time. Requests which exceed this number are dropped and are not quarantined.
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.
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.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
SMP.AUTO_ENABLE.int	1	<p>Automatically registers or de-registers Symantec DLP Agents with Symantec Management Platform (SMP). Change this setting if you do not want Symantec DLP Agents to be registered on SMP.</p> <p>A setting of 0 disables the feature.</p> <p>A setting of 1 enables the feature and automatically registers Symantec DLP Agents with SMP.</p> <p>A setting of 2 enables the feature and automatically de-registers Symantec DLP Agents from SMP.</p> <p>Make sure to set this parameter to 0 if registration or un-registration is being carried out by a registration utility or an SMP registration policy. Otherwise, the Symantec DLP Agent automatically resets the registration operation.</p>
ServerCommunication.CONNECTION_INTERVAL_SECONDS	86400	The default amount of time between successful connection attempts, in seconds.
ServerCommunication.CONNECTION_RETRY_ATTEMPTS.int	10	The maximum number of times a DLP agent tries to connect to the Endpoint Server.
ServerCommunication.CONNECTION_RETRY_INTERVAL_SECONDS.int	10	The amount of time in between failed connection attempts for the DLP agent to try to connect to the Endpoint Server.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
ServerCommunication.CONNECT_WHEN_IP_CHANGES.int	1	If the IP address of the Endpoint Server changes, the DLP agent tries to connect to the server and re-acquire policy information. If you enter a 1 in this setting, the DLP agent automatically tries to reconnect with the server. If a 0 is entered, the DLP agent does not try to reconnect with the server.
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	Maximum amount of time, in seconds, the agent waits between connection retries to the same Endpoint Server.
UI.BUTTON_OK.str	OK	This setting controls the text on the OK button. Change this setting if you use a locale that is not supported. The default setting is English.
UI.BUTTON_OKTOALL.str	OK To All	This setting controls the text on the OK To All button. Change this setting if you use a locale that is not supported. The default setting is English.
UI.CONSECUTIVE_TRANSACTION_TIME.str	10	Maximum time, in seconds, in between two file operations to be considered as a single transaction.
UI.MONITOR_MSG_TITLE.str		The message title for a notification pop-up message.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
UI.MONITOR_TITLEBAR.str	Warning	This setting 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.NO_SCAN.int	0	If any number other than zero, the scan dialog is not displayed.
UI.NWC_EVENT_LIMIT_FS.int	5	The maximum number of events that can be queued before accepting a default action for further incidents. 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 accepting a default action for further incidents. 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.
UI.PREVENT_MSG_TITLE.str		Message title for a block pop-up message.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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	This setting controls the static title message in the title bar for the Endpoint block notification pop-up dialog box. Change this setting if you use a locale that is not supported. The default setting is English.
UI.PREVENT_WINPOSITION.int	0	Start position of the Prevent dialog window.
UI.QUARANTINE_PROMPT.str	The file is quarantined at:	This setting controls the text that specifies where the quarantined data is located. Change this setting if you use a locale that is not supported. The default setting is in English.
UI.SCAN_BAR.str		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 computer.
UI.SCAN_DELAY.int	0	The amount of time 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. The default setting is 0.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
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. The default setting is 0.
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. The default setting is 0.
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. The default setting is 0.
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. The default setting is 0.
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. The default setting is 1, which allows monitoring.
UI.SCAN_SHOWTIME.int	2	Minimum time, in seconds, for the scan dialog to remain on the screen.

**Table 10-8** Agent advanced settings (*continued*)

Name of Setting	Default values	Description
UI.SCAN_TITLE.str		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 computer.
UI.USERINPUT_PROMPT.str	Others:	This setting 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.



# 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 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 (Email) Server communicates with a specific MTA on your network. See [“Operational log files”](#) on page 226.
- 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 228.

- 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\Vontu\.install4j\installation.log` stores the installation log for Symantec Data Loss Prevention.
  - `installdir\oracle_home\admin\protect\` stores the installation log for Oracle 10g.

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 `\Vontu\Protect\logs\` directory on Windows installations and in the `/var/log/Vontu/` 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
<code>boxmonitor_operational_0.log</code>	<p>The <code>BoxMonitor</code> process oversees the detection server processes that pertain to that particular server type.</p> <p>For example, the processes that run on Network Monitor are file reader and packet capture.</p> <p>The <code>BoxMonitor</code> log file is typically very small, and it shows how the application processes are running.</p>	All detection servers

**Table 11-1** Operational log files (*continued*)

Log file name	Description	Server
detection_operational_0.log	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: <ul style="list-style-type: none"> <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>	All detection servers
manager_operational.log.0	Logs information about the Symantec Data Loss Prevention manager process, which implements the Enforce Server administration console user interface.	Enforce 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
SmtpPrevent0.log	This operational log file pertains to SMTP Prevent only. It is the primary log for tracking the health and activity of a Network Prevent (Email) system. Examine this file for information about the communication between the MTAs and the detection server.	SMTP Prevent detection servers

**Table 11-1** Operational log files (*continued*)

Log file name	Description	Server
WebPrevent_Access0.log	This access log file pertains to Web Prevent only. It records all the requests that Web Prevent processes. It is similar to Web access logs for a proxy server.	Web Prevent detection servers
WebPrevent_Operational0.log	This operational log file pertains to Web Prevent only. It reports the operating condition of Web Prevent such as whether the system is up or down, connection management, and so on. This log is the primary log file for tracking Web Prevent operations.	Web Prevent detection servers
webservices_access0.log	This log file records successful and failed attempts to access the reporting Web Service.	Enforce Server
webservices_soap0.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 <i>Symantec Data Loss Prevention Reporting API Developers Guide</i> for more information.	Enforce server

See [“Network Prevent \(Web\) operational log files and event codes”](#) on page 241.

See [“Network Prevent \(Web\) access log files and fields”](#) on page 243.

See [“Network Prevent \(Email\) log levels”](#) on page 245.

See [“Network Prevent \(Email\) operational log codes”](#) on page 246.

See [“Network Prevent \(Email\) originated responses and codes”](#) on page 249.

## Debug log files

The Enforce Server and the detection servers store debug log files in the `\Vontu\Protect\logs\` directory on Windows installations and in the

`/var/log/Vontu/` directory on Linux installations. A number at the end of the log file name indicates the count (shown as 0 in [Table 11-2](#)).

[Table 11-2](#) lists and describes the Symantec Data Loss Prevention debug log files.

**Table 11-2** Debug log files

Log file name	Description	Server
Aggregator0.log	<p>This file describes communications between the detection server and the agents.</p> <p>Look at this log to troubleshoot the following problems:</p> <ul style="list-style-type: none"> <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>	Endpoint detection servers
BoxMonitor0.log	<p>This file is typically very small, and it shows how the application processes are running. The <code>BoxMonitor</code> process oversees the detection server processes that pertain to that particular server type.</p> <p>For example, the processes that run on Network Monitor are file reader and packet capture.</p>	All detection servers
ContentExtractor0.log	<p>This log file may be helpful for troubleshooting <code>ContextExtractor</code> issues.</p>	All detection servers, Enforce Server
DiscoverNative.log.0	<p>Contains the log statements that the Network Discover native code emits. Currently contains the information that is related to <code>.pst</code> scanning. This log file applies only to the Network Discover Servers that run on Windows platforms.</p>	Discover detection servers
FileReader0.log	<p>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. Look at this log file to find out why an incident was not detected. One symptom that shows up is content extractor timeouts.</p>	All detection servers
IncidentPersister0.log	<p>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.</p>	Enforce Server

Table 11-2 Debug log files (continued)

Log file name	Description	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
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 <code>drop_pcap</code> directory. Look at this log if there is a problem with dropped packets or traffic is lower than expected. <code>PacketCapture</code> 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 <code>PacketCapture</code> communications.	Network Monitor
RequestProcessor0.log	This log file pertains to SMTP Prevent only. The log file is primarily for use in cases where <code>Smtpprevent0.log</code> is not sufficient.	SMTP Prevent detection servers
ScanDetail- <i>target</i> -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: <code>stdout</code> and <code>stderr</code> only (fatal events).	Enforce Server

**Table 11-2**      Debug log files (*continued*)

Log file name	Description	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 Prevent \(Web\) protocol debug log files](#)” on page 244.

See “[Network Prevent \(Email\) log levels](#)” on page 245.

## 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 236.
- **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 server.  
 See “[Configuring server logging behavior](#)” on page 231.

See “[About log files](#)” on page 225.

## 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 151.

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 filenames correspond to an actual logging configuration filenames.
- Root level logging is enabled in the configuration file. This 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
<b>Restore Defaults</b>	Restores log file parameters to their default values.
<b>Reporting API SOAP Logging</b>	<p>Logs the entire SOAP request and response message for most requests to the Reporting API Web Service. The logged messages are stored in the <code>webservices_soap.log</code> file, which is not created by default with new installations.</p> <p>You can use the contents of <code>webservices_soap.log</code> 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.</p>
<b>Custom Attribute Lookup Logging</b>	<p>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 (<code>c:\Vontu\logs\tomcat\localhost.date.log</code>) and the <code>IncidentPersister_0.log</code> file.</p> <p>See <a href="#">“About custom attributes”</a> on page 797.</p>

**Table 11-4** Preconfigured log settings for detection servers

Select a Diagnostic Log Setting value	Detection server uses	Description
<b>Restore Defaults</b>	All detection servers	Restores log file parameters to their default values.
<b>Discover Trace Logging</b>	Network Discover servers	Enables informational logging for Network Discover scans. These log messages are stored in <code>FileReader0.log</code> .

**Table 11-4** Preconfigured log settings for detection servers (*continued*)

Select a Diagnostic Log Setting value	Detection server uses	Description
<b>Detection Trace Logging</b>	All detection servers	<p>Logs information about each message that the detection server processes. This includes information such as:</p> <ul style="list-style-type: none"> <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> <p>When you enable <b>Detection Trace Logging</b>, the resulting messages are stored in the <code>detection_operational_trace_0.log</code> file.</p> <p><b>Note:</b> 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.</p>
<b>Packet Capture Debug Logging</b>	Network Monitor servers	<p>Enables basic debug logging for packet capture with Network Monitor. This setting logs information in the <code>PacketCapture.log</code> file.</p> <p>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.</p> <p>If you apply this log configuration setting to a server, you must restart the server process to enable the change.</p>

**Table 11-4**      Preconfigured log settings for detection servers (*continued*)

Select a Diagnostic Log Setting value	Detection server uses	Description
<b>Email Prevent Logging</b>	Network Prevent (Email) servers	<p>Enables full message logging for Network Prevent (Email) servers. This setting logs the complete message content and includes execution and error tracing information. Logged information is stored in the <code>Smtpprevent0.log</code> file.</p> <p><b>Note:</b> 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.</p> <p>See <a href="#">“Network Prevent (Email) operational log codes”</a> on page 246.</p> <p>See <a href="#">“Network Prevent (Email) originated responses and codes”</a> on page 249.</p>
<b>ICAP Prevent Message Processing Logging</b>	Network Prevent (Web) servers	<p>Enables operational and access logging for Network Prevent (Web). This setting logs information in the <code>FileReader0.log</code> file.</p> <p>See <a href="#">“Network Prevent (Web) operational log files and event codes”</a> on page 241.</p> <p>See <a href="#">“Network Prevent (Web) access log files and fields”</a> on page 243.</p>

Follow this procedure to change the log configuration for a Symantec Data Loss Prevention server.

**To configure logging properties for a server**

- 1** Click the **Configuration** tab if it is not already selected.
- 2** If you want to configure logging properties for a detection server, select the server name from the **Select a Detection Server** menu.

- 3 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.

- 4 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**.

---

- 5 Click **Configure Logs** to apply the preconfigured setting or custom log configuration file to the selected server.
- 6 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 231.

## 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
<b>Operational Logs</b>	<p>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.</p> <p>For example, you can use operational log files to verify that a Network Prevent (Email) Server communicates with a specific MTA on your network.</p>
<b>Debug and Trace Logs</b>	<p>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.</p>

**Table 11-5** File types for collection (*continued*)

File type	Description
<p><b>Configuration Files</b></p>	<p>Use the <b>Configuration Files</b> option to retrieve both logging configuration files and server feature configuration files.</p> <p>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.</p> <p>For example, by default the Enforce console does not log SOAP messages that are generated from Reporting API Web service clients. The <code>ManagerLogging.properties</code> file contains a property that enables logging for SOAP messages.</p> <p>You can modify many common logging configuration properties by using the presets that are available on the <b>Configuration</b> tab.</p> <p>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.</p> <p>See <a href="#">“Configuring server logging behavior”</a> on page 231.</p> <p>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 server’s communication settings. 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.</p>

**Table 11-5** File types for collection (*continued*)

File type	Description
<b>Agent Logs</b>	<p>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.</p> <p>Use the agent overview 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.</p> <p>When the logs are pulled from the endpoint computer, 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 computer at a time.</p> <p>See <a href="#">“Agent overview actions”</a> on page 1122.</p> <p>See <a href="#">“Using the agents overview screen”</a> on page 1117.</p>

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.
- 2 Use the **Date Range** menu to select a range of dates for the files you want to 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.
- 3 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.
- 4 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.
- 7 To download collected logs to your local computer, click **Download** next to the log collection entry.
- 8 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 231.

See [“About log files”](#) on page 225.

## 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 Prevent \(Web\) operational log files and event codes”](#) on page 241.
- See [“Network Prevent \(Email\) operational log codes”](#) on page 246.
- See [“Network Prevent \(Email\) originated responses and codes”](#) on page 249.

## Network Prevent (Web) operational log files and event codes

Network Prevent (Web) log file names use the format of `WebPrevent_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. This file is in the `Vontu\Protect\config` directory. By default, the values are:

- `com.vontu.icap.log.IcapOperationalLogHandler.limit = 5000000`
- `com.vontu.icap.log.IcapOperationalLogHandler.count = 5`

[Table 11-6](#) lists the Network Prevent (Web) defined operational logging codes by category. The italicized part of the text contains event parameters.

**Table 11-6** Status codes for Network Prevent (Web) operational logs

Code	Text and Description
Operational Events	
1100	Starting Network Prevent (Web)
1101	Shutting down Network Prevent (Web)
Connectivity Events	

**Table 11-6** Status codes for Network Prevent (Web) operational logs (*continued*)

Code	Text and Description
1200	<p>Listening for incoming connections at <i>icap_bind_address:icap_bind_port</i></p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <i>icap_bind_address</i> is the Network Prevent (Web) bind address to which the server listens. This address is specified with the Icap.BindAddress Advanced Setting.</li> <li>■ <i>icap_bind_port</i> is the port at which the server listens. This port is set in the <b>Server &gt; Configure</b> page.</li> </ul>
1201	<p>Connection (<i>id=conn_id</i>) opened from <i>host(icap_client_ip:icap_client_port)</i></p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <i>conn_id</i> is the connection ID that is allocated to this connection. This ID can be helpful in doing correlations between multiple logs.</li> <li>■ <i>icap_client_ip</i> and <i>icap_client_port</i> are the proxy's IP address and port from which the connect operation to Network Prevent (Web) was performed.</li> </ul>
1202	<p>Connection (<i>id=conn_id</i>) closed (<i>close_reason</i>)</p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <i>conn_id</i> is the connection ID that is allocated to the connect operation.</li> <li>■ <i>close_reason</i> provides the reason for closing the connection.</li> </ul>
1203	<p>Connection states: REQMOD=<i>N</i>, RESPMOD=<i>N</i>,  OPTIONS=<i>N</i>, OTHERS=<i>N</i></p> <p>Where <i>N</i> indicates the number of connections in each state, when the message was logged.</p> <p>This message provides the system state in terms of connection management. It is logged whenever a connection is opened or closed.</p>
<b>Connectivity Errors</b>	
5200	<p>Failed to create listener at <i>icap_bind_address:icap_bind_port</i></p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <i>icap_bind_address</i> is the Network Prevent (Web) bind address to which the server listens. This address can be specified with the Icap.BindAddress Advanced Setting.</li> <li>■ <i>icap_bind_port</i> is the port at which the server listens. This port is set on the <b>Server &gt; Configure</b> page.</li> </ul>

**Table 11-6** Status codes for Network Prevent (Web) operational logs (*continued*)

Code	Text and Description
5201	<p>Connection was rejected from unauthorized host (<i>host_ip:port</i>)</p> <p>Where <i>host_ip</i> and <i>port</i> are the proxy system IP and port address from which a connect attempt to Network Prevent (Web) was performed. If the host is not listed in the Icap.AllowHosts Advanced setting, it is unable to form a connection.</p>

See “[About log files](#)” on page 225.

## Network Prevent (Web) access log files and fields

Network Prevent (Web) log file names use the format of `WebPrevent_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.icap.log.IcapAccessLogHandler.limit = 5000000`
- `com.vontu.icap.log.IcapAccessLogHandler.count = 5`

A Network Prevent (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
```

**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 Prevent (Web) access log fields

Fields	Explanation
<code>host_ip</code>	IP address of the host that made the request.
<code>auth_user</code>	Authorized user for this request.

**Table 11-7** Network Prevent (Web) access log fields (*continued*)

Fields	Explanation
time_stamp	Time that Network Prevent (Web) receives the request.
request_line	Line that represents the request.
icap_status_code	ICAP response code that Network Prevent (Web) sends by for this request.
request_size	Request size in bytes.
referer	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 (microsecond)	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 Prevent (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.
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.

See “[About log files](#)” on page 225.

## Network Prevent (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. The Network Prevent (Web) 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 225.

## Network Prevent (Email) log levels

Network Prevent (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 `Vontu\Protect\config` directory. For example, `com.vontu.mta.rp.level = FINE` specifies the FINE level of detail.

[Table 11-8](#) describes the Network Prevent (Email) log levels.

**Table 11-8** Network Prevent (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 225.

## Network Prevent (Email) operational log codes

[Table 11-9](#) lists the defined Network Prevent (Email) operational logging codes by category.

**Table 11-9** Status codes for Network Prevent (Email) operational log

Code	Description
<b>Core Events</b>	
1100	Starting Network Prevent (Email)
1101	Shutting down Network Prevent (Email)
1102	Reconnecting to FileReader (tid= <i>id</i> )  Where <i>id</i> is the thread identifier.  The RequestProcessor attempts to re-establish its connection with the FileReader for detection.
1103	Reconnected to the FileReader successfully (tid= <i>id</i> )  The RequestProcessor was able to re-establish its connection to the FileReader.
<b>Core Errors</b>	
5100	Could not connect to the FileReader (tid= <i>id</i> timeout=.3s)  An attempt to re-connect to the FileReader failed.
5101	FileReader connection lost (tid= <i>id</i> )  The RequestProcessor connection to the FileReader was lost.
<b>Connectivity Events</b>	
1200	Listening for incoming connections (local= <i>hostname</i> )  <i>Hostnames</i> is an IP address or fully-qualified domain name.
1201	Connection accepted (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> )  Where <i>N</i> is the connection identifier.
1202	Peer disconnected (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> )

**Table 11-9** Status codes for Network Prevent (Email) operational log (*continued*)

Code	Description
1203	Forward connection established (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> )
1204	Forward connection closed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> )
1205	Service connection closed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> messages=1 time=0.14s)
<b>Connectivity Errors</b>	
5200	Connection is rejected from the unauthorized host (tid= <i>id</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> )
5201	Local connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i> )
5202	Sender connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i> )
5203	Forwarding connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i> )
5204	Peer disconnected unexpectedly (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i> )
5205	Could not create listener (address=local= <i>hostname:port</i> reason= <i>Explanation</i> )
5206	Authorized MTAs contains invalid hosts: <i>hostname</i> , <i>hostname</i> , ...

**Table 11-9** Status codes for Network Prevent (Email) operational log (*continued*)

Code	Description
5207	MTA restrictions are active, but no MTAs are authorized to communicate with this host
5208	TLS handshake failed (reason= <i>Explanation</i> tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i> )
5209	TLS handshake completed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i> )
5210	All forward hosts unavailable (tid= <i>id</i> cid= <i>N</i> reason= <i>Explanation</i> )
5211	DNS lookup failure (tid= <i>id</i> cid= <i>N</i> NextHop= <i>hostname</i> reason= <i>Explanation</i> )
5303	Failed to encrypt incoming message (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i> )
5304	Failed to decrypt outgoing message (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i> )
<b>Message Events</b>	

**Table 11-9** Status codes for Network Prevent (Email) operational log (*continued*)

Code	Description
1300	<p>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)</p> <p>Where:</p> <ul style="list-style-type: none"> <li>■ Recipient_count is the total number of addressees in the To, CC, and BCC fields.</li> <li>■ Response is the Network Prevent (Email) response which can be one of: PASS, BLOCK, BLOCK_AND_REDIRECT, REDIRECT, MODIFY, or ERROR.</li> <li>■ Thee status is an Enhanced Status code. See “<a href="#">Network Prevent (Email) originated responses and codes</a>” on page 249.</li> <li>■ The rtime is the time in seconds for Network Prevent (Email) to fully receive the message from the sending MTA.</li> <li>■ The dtime is the time in seconds for Network Prevent (Email) to perform detection on the message.</li> <li>■ The mtime is the total time in seconds for Network Prevent (Email) to process the message Message Errors.</li> </ul>
<b>Message Errors</b>	
5300	<p>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)</p> <p>Where <i>header_ID</i> is an RFC 822 Message-Id header if one exists.</p>
5301	Sender rejected during re-submit
5302	Recipient rejected during re-submit

See “[About log files](#)” on page 225.

## Network Prevent (Email) originated responses and codes

Network Prevent (Email) originates the following responses. Other protocol responses are expected as Network Prevent (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 Prevent generates a specific response to an event that is not relayed from downstream.

“Enhanced Status” is the RFC1893 Enhanced Status Code associated with the response.

**Table 11-10** Network Prevent (Email) originated responses

Code	Enhanced Status	Text	Description
250	2.0.0	Ok: Carry on.	Success code that Network Prevent (Email) uses.
221	2.0.0	Service closing.	The normal connection termination code that Network Prevent (Email) generates if a QUIT request is received when no forward MTA connection is active.
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.

**Table 11-10** Network Prevent (Email) originated responses (*continued*)

Code	Enhanced Status	Text	Description
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.
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 (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 225.

# 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 sslkeytool utility and server certificates](#)
- [About the SQL Preindexer](#)
- [About the Remote EDM Indexer](#)

## 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	<p>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.</p> <p>See <a href="#">“About the Environment Check Utility”</a> on page 256.</p>
Log Collection Utility	<p>Collects the log files from a single Symantec Data Loss Prevention server. The utility archives the log files into a ZIP file, which Symantec Support can use to troubleshoot problems. This utility is executed as an option to the Environment Check Utility.</p> <p><b>Note:</b> The Log Collection Utility gathers log files only from the local server on which you run the utility. To collect log files from any or all servers in a Symantec Data Loss Prevention deployment, use the log collection screen of the Enforce Server administration console (<b>System &gt; Servers &gt; Logs</b>). See the Enforce Server administration console online Help for more information.</p>
DBPasswordChanger	<p>Changes the encrypted password that the Enforce Server uses to connect to the Oracle database.</p> <p>See <a href="#">“About DBPasswordChanger”</a> on page 258.</p>
sslkeytool	<p>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.</p> <p>See <a href="#">“About the sslkeytool utility and server certificates”</a> on page 260.</p>

**Table 12-1** Symantec Data Loss Prevention utilities (*continued*)

Name	Description
SQL Preindexer	Indexes an SQL database or runs a 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 <a href="#">“About the SQL Preindexer”</a> on page 265.
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 <a href="#">“About the Remote EDM Indexer”</a> on page 268.

## About Endpoint utilities

[Table 12-2](#) describes those utilities that apply to the Endpoint products.  
See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.

**Table 12-2** Endpoint utilities

Name	Description
endpointkeytool	The endpointkeytool utility creates a new authentication key that is used to encrypt communication between the Endpoint Server and the Symantec DLP Agent. The new authentication key replaces the hard-coded AES key. Use endpointkeytool to generate a new authentication key before installing the Symantec DLP Agent on endpoint computers.

**Table 12-2** Endpoint utilities (*continued*)

Name	Description
Service_Shutdown.exe	This utility enables an administrator to turn off both the agent and the watchdog services on an endpoint computer. (As a tamper-proofing measure, it is not possible for a user to stop either the agent or the watchdog service.)
vontu_sqlite3.exe	This utility provides a 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.
logdump.exe	This tool lets you view the Symantec DLP Agent extended log files, which are hidden for security reasons.

## 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 style="list-style-type: none"> <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

**Table 12-3** Environment Check Utility tasks (*continued*)

Task	Server Type
<ul style="list-style-type: none"> <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 <code>/Vontu/Protect/ECU/eculogs/monitorSettings</code> 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:\Vontu\Protect\ECU` directory.

### To run the ECU on Windows

- 1 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:\Vontu\Protect\ECU` if you installed in the default location).
- 3 Execute the utility:

```
EnvironmentCheckUtility.exe
```

See [“About Environment Check Utility output”](#) on page 258.

## Running the Environment Check Utility on Linux

If the default installation directory was used, the Environment Check Utility is located in the `/opt/Vontu/Protect/ECU` directory.

### To run the ECU on Linux

- 1 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/Vontu/Protect/ECU
```

- 3 Execute the utility:

```
./EnvironmentCheckUtility
```

See [“About Environment Check Utility output”](#) on page 258.

## 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 `eculogs.zip` 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 225.

## About DBPasswordChanger

Symantec Data Loss Prevention stores encrypted passwords to the Oracle database in a file that is called `ProtectPassword.properties`, located in

c:\Vontu\Protect\config (Windows) or /opt/Vontu/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 259.

## DBPasswordChanger syntax

The DBPasswordChanger utility uses the following syntax:

```
DBPasswordChanger password_file administrator_password
new_oracle_password
```

All command-line parameters are required. The following table describes each command-line parameter.

See “[Example of using DBPasswordChanger](#)” on page 259.

**Table 12-4** DBPasswordChanger command-line parameters

Parameter	Description
<i>password_file</i>	Specifies the file that contains the encrypted password. By default, this file is named <code>ProtectPassword.properties</code> and is stored in <code>\Vontu\Protect\config</code> (Windows) or <code>/opt/Vontu/Protect/config</code> (Linux).
<i>administrator_password</i>	Specifies the password of the Symantec Data Loss Prevention administrator. A valid administrator password is required to change the encrypted Oracle password.
<i>new_oracle_password</i>	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\ProtectPassword.properties  
protect_symantec protect_oracle
```

See “[DBPasswordChanger syntax](#)” on page 259.

## About the `sslkeytool` utility and server certificates

Symantec Data Loss Prevention uses Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt all data that is transmitted between servers. Symantec Data Loss Prevention also uses the SSL/TLS protocol for mutual authentication between servers. Servers implement authentication by the mandatory use of client and server-side certificates. By default, connections between servers use a single, self-signed certificate that is embedded securely inside the Symantec Data Loss Prevention software. All Symantec Data Loss Prevention installations at all customer sites use this same certificate.

Symantec recommends that you replace the default certificate with unique, self-signed certificates for your organization’s installation. You store a certificate on the Enforce Server, and on each detection server that communicates with the Enforce Server. These certificates are generated with the `sslkeytool` utility.

---

**Note:** If you install a Network Prevent detection server in a hosted environment, you must generate unique certificates for your Symantec Data Loss Prevention servers. You cannot use the built-in certificate to communicate with a hosted Network Prevent server.

---

---

**Note:** Symantec recommends that you create dedicated certificates for communication with your Symantec Data Loss Prevention servers. When you configure the Enforce Server to use a generated certificate, all detection servers in your installation must also use generated certificates. You cannot use the built-in certificate with some detection servers and the built-in certificate with other servers.

---

See “[About `sslkeytool` command line options](#)” on page 261.

See “[Using `sslkeytool` to generate new Enforce and detection server certificates](#)” on page 262.

See “[Using `sslkeytool` to add new detection server certificates](#)” on page 264.

## About `sslkeytool` command line options

`sslkeytool` is a command-line utility that generates a unique pair of SSL certificates (keystore files). `sslkeytool` is located in the `\Vontu\Protect\bin` directory (Windows) or `/opt/Vontu/Protect/bin` directory (Linux). It must run under the Symantec Data Loss Prevention operating system user account which, by default, is “protect.” Also, you must run `sslkeytool` directly on the Enforce server computer.

The following command forms and options are available for `sslkeytool`:

- `-genkey [-dir=directory -alias=aliasFile]`  
Generates two unique certificates (keystore files) by default: one for the Enforce Server and one for other detection servers. The optional `-dir` argument specifies the directory where the keystore files are placed. The optional `-alias` argument generates additional keystore files for each alias specified in the *aliasFile*. You can use the alias file to generate unique certificates for each detection server in your system (rather than using a same certificate on each detection server). Use this command form the first time you generate unique certificates for your Symantec Data Loss Prevention installation.
- `-list=file`  
Lists the content of the specified keystore file.
- `-alias=aliasFile -enforce=enforceKeystoreFile [-dir=directory]`  
Generates multiple certificate files for detection servers using the aliases you define in *aliasFile*. You must specify an existing Enforce Server keystore file to use when generating the new detection server keystore files. The optional `-dir` argument specifies the directory where the keystore files are placed. If you specify the `-dir` argument, you must also place the Enforce Server keystore file in the specified directory. Use this command form to add new detection server certificates to an existing Symantec Data Loss Prevention installation.

For example, the command `sslkeytool -genkey` generates two files:

- `enforce.timestamp.sslKeyStore`
- `monitor.timestamp.sslKeyStore`

Unless you specified a different directory with the `-dir` argument, these two keystore files are created in the `bin` directory where the `sslkeytool` utility resides.

See [“About the `sslkeytool` utility and server certificates”](#) on page 260.

See [“Using `sslkeytool` to generate new Enforce and detection server certificates”](#) on page 262.

See [“Using `sslkeytool` to add new detection server certificates”](#) on page 264.

## Using `sslkeytool` to generate new Enforce and detection server certificates

After installing Symantec Data Loss Prevention, use the `-genkey` argument with `sslkeytool` to generate new certificates for the Enforce Server and detection servers. Symantec recommends that you replace the default certificate used to secure communication between servers with unique, self-signed certificates. The `-genkey` argument automatically generates two certificate files. You store one certificate on the Enforce Server, and the second certificate on each detection server. The optional `-alias` command lets you generate a unique certificate file for each detection server in your system. To use the `-alias` you must first create an alias file that lists the name of each alias create.

### To generate unique certificates for Symantec Data Loss Prevention servers

- 1 Log on to the Enforce Server computer using the "protect" user account you created during Symantec Data Loss Prevention installation.
- 2 From a command window, go to the `c:\Vontu\Protect\bin` directory where the `sslkeytool` utility is stored.
- 3 If you want to create a dedicated certificate file for each detection server, first create a text file to list the alias names you want to create. Place each alias on a separate line. For example:

```
net_monitor01
protect01
endpoint01
smtp_prevent01
web_prevent01
classification01
```

---

**Note:** The `-genkey` argument automatically creates certificates for the "enforce" and "monitor" aliases. Do not add these aliases to your custom alias file.

---

- 4 Run the `sslkeytool` utility with the `-genkey` argument and optional `-dir` argument to specify the output directory. If you created a custom alias file, also specify the optional `-alias` argument, as in this example:

This generates new certificates (keystore files) in the specified directory. Two files are automatically generated with the `-genkey` argument:

- `enforce.timestamp.sslKeyStore`
- `monitor.timestamp.sslKeyStore`

`sslkeytool` also generates individual files for any aliases that are defined in the alias file. For example:

- `net_monitor01.timestamp.sslKeyStore`
- `protect01.timestamp.sslKeyStore`
- `endpoint01.timestamp.sslKeyStore`
- `smtp_prevent01.timestamp.sslKeyStore`
- `web_prevent01.timestamp.sslKeyStore`
- `classification01.timestamp.sslKeyStore`

- 5 Copy the certificate file whose name begins with `enforce` to the `c:\Vontu\Protect\keystore` directory on the Enforce Server.
- 6 If you want to use the same certificate file with all detection servers, copy the certificate file whose name begins with `monitor` to the `c:\Vontu\Protect\keystore` directory of each detection server in your system.  
  
If you generated a unique certificate file for each detection server in your system, copy the appropriate certificate file to the `keystore` directory on each detection server computer.
- 7 Delete or secure any additional copies of the certificate files to prevent unauthorized access to the generated keys.
- 8 Restart the Vontu Monitor Controller service on the Enforce Server and the Vontu Monitor service on the detection servers.

When you install a Symantec Data Loss Prevention server, the installation program creates a default keystore in the `keystore` directory. When you copy a generated certificate file into this directory, the generated file overrides the default certificate. If you later remove the certificate file from the keystore directory, Symantec Data Loss Prevention reverts to the default keystore file embedded within the application. This behavior ensures that data traffic is always protected. Note, however, that you cannot use the built-in certificate with certain servers and a generated certificate with other servers. All servers in the Symantec Data Loss Prevention system must use either the built-in certificate or a custom certificate.

---

**Note:** If more than one keystore file is placed in the keystore directory, the server does not start.

---

See [“Using `sslkeytool` to add new detection server certificates”](#) on page 264.

See [“About `sslkeytool` command line options”](#) on page 261.

See [“About the `sslkeytool` utility and server certificates”](#) on page 260.

## Using `sslkeytool` to add new detection server certificates

Use `sslkeytool` with the `-alias` argument to generate new certificate files for an existing Symantec Data Loss Prevention deployment. When you use this command form, you must provide the current Enforce Server keystore file, so that `sslkeytool` can embed the Enforce Server certificate in the new detection server certificate files that you generate.

### To generate new detection server certificates

- 1 Log on to the Enforce Server computer using the "protect" user account that you created during Symantec Data Loss Prevention installation.
- 2 From a command window, go to the `c:\Vontu\Protect\bin` directory where the `sslkeytool` utility is stored.
- 3 Create a directory in which you will store the new detection server certificate files. For example:

```
mkdir new_certificates
```

- 4 Copy the Enforce Server certificate file to the new directory. For example:
- 5 Create a text file that lists the new server alias names that you want to create. Place each alias on a separate line. For example:

```
endpoint02  
smtp_prevent02
```

- 6 Run the `sslkeytool` utility with the `-alias` argument and `-dir` argument to specify the output directory. Also specify the name of the Enforce Server certificate file that you copied into the certificate directory. For example:

This generates a new certificate file for each alias, and stores the new files in the specified directory. Each certificate file also includes the Enforce Server certificate from the Enforce keystore that you specify.

- 7 Copy each new certificate file to the `c:\Vontu\Protect\keystore` directory on the appropriate detection server computer.
- 8 Delete or secure any additional copies of the certificate files to prevent unauthorized access to the generated keys.
- 9 Restart the Vontu Monitor service on each detection server to use the new certificate file.

## Verifying server certificate usage

Symantec Data Loss Prevention uses system events to indicate whether servers are using the built-in certificate or user-generated certificates to secure communication. If servers use the default, built-in certificate, Symantec Data Loss Prevention generates a warning event. If servers use generated certificates, Symantec Data Loss Prevention generates an info event.

Symantec recommends that you use generated certificates, rather than the built-in certificate, for added security.

If you install Network Prevent to a hosted environment, you cannot use the built-in certificate and you must generate and use unique certificates for the Enforce Server and detection servers.

### To determine the type of certificates that Symantec Data Loss Prevention uses

- 1 Start the Enforce Server or restart the Vontu Monitor Controller service on the Enforce Server computer.
- 2 Start each detection server or restart the Vontu Monitor service on each detection server computer.
- 3 Log in to the Enforce Server administration console.
- 4 Select **System > Servers > Alerts**.
- 5 Check the list of alerts to determine the type certificates that Symantec Data Loss Prevention servers use:
  - If servers use the built-in certificate, the Enforce Server shows a warning event with code 2709: Using built-in certificate.
  - If servers use unique, generated certificates, the Enforce Server shows an info event with code 2710: Using user generated certificate.

## About the SQL Preindexer

This chapter describes how to use the SQL Preindexer. The SQL Preindexer utility is always used with the Remote EDM Indexer utility. It is installed in the `\Vontu\Protect\bin` directory during installation of the Remote EDM Indexer. The SQL Preindexer utility generates an index directly from a SQL database. It processes the database query and then pipes it to the Remote EDM Indexer utility.

Read the chapter about the Remote EDM Indexer in this guide before running the SQL Preindexer.

See [“About the Remote EDM Indexer”](#) on page 268.

The SQL Preindexer runs from the command line. If you are on Linux, change users to the “protect” user before running the SQL Preindexer. (The installation program creates the “protect” user.) The SQL Preindexer only supports Oracle databases.

An example of a command to run the SQL Preindexer follows. The SQL Preindexer runs a SQL query to capture the name and the salary data from the employee data table in the Oracle database. This example shows how to pipe the output of the SQL query to the Remote EDM Indexer. The Remote EDM Indexer indexes the results using the `ExportEDMProfile.edm` profile. The generated index files are stored in the `EDMIndexDirectory` folder.

```
SqlPreindexer -alias=@//myhost:1521/orcl -username=scott -password=tiger -query="SELECT  
name, salary FROM employee" | RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm  
-result=C:\EDMIndexDirectory\
```

Because you pipe the output from the SQL Preindexer to the Remote EDM Indexer, review the section about Remote EDM Indexer command functions and options.

See [Table 12-2](#) on page 255.

## SQL Preindexer command function and options

The SQL Preindexer requires the `-alias` option and the `-username` option. All of the command options for the SQL Preindexer are described in the following table. If you omit the `-query` option, the utility indexes the entire database.

The SQL Preindexer command has the following options:

<code>-alias</code>	Specifies the database alias used to connect to the database in the following format: <code>@//localhost:port/sid</code> For example: <code>@//myhost:1521/orcl</code> This option is required.
<code>-driver</code>	Specifies the JDBC driver class (for example, <code>oracle.jdbc.driver.OracleDriver</code> ).
<code>-encoding</code>	Specifies the character encoding of the data to index. The default is <code>iso-8859-1</code> , but data with non-English characters should use <code>UTF-8</code> or <code>UTF-16</code> .
<code>-password</code>	Specifies the password to the database. If this option is not specified, the password is read from <code>stdin</code> .
<code>-query</code>	Specifies the SQL query to run.

<code>-query_path</code>	Specifies the file path that contains a SQL query to run. This option can be used as an alternative to <code>-query</code> when the query is a long SQL statement.
<code>-separator</code>	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 character in quotation marks as in <code>"</code> , <code>" </code> , or <code>" "</code> .
<code>-subprotocol</code>	Specifies the JDBC connect string subprotocol (for example, <code>oracle:thin</code> ).
<code>-username</code>	Specifies the name of the database user. This option is required.
<code>-verbose</code>	Displays a statistical summation of the indexing operation when the index is complete.

See [“Troubleshooting preindexing errors”](#) on page 267.

## Troubleshooting preindexing errors

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

- 1 Locate the `Indexer.properties` file at `\Program Files\Vontu\Protect\config\Indexer.properties` (Windows) or `/opt/Vontu/Protect/confide/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.”
- 4 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 265.

## About the Remote EDM Indexer

The Remote EDM Indexer is a utility that converts a comma-separated value, or tab-delimited, data file to an Exact Data Matching 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.

The SQL Preindexer is often used with the Remote EDM Indexer. The SQL Preindexer is used to run SQL queries against SQL databases and pass the resulting data to the Remote EDM Indexer.

See [“About the SQL Preindexer”](#) on page 265.

See [“Using the Remote EDM Indexer”](#) on page 269.

See [“About implementing Exact Data Matching”](#) on page 368.

## System requirements for the Remote EDM Indexer

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 requirements.

The RAM requirements for the Remote EDM Indexer vary according to the size of the data files being indexed. Data files with less than a million rows of records

can be indexed from an average desktop computer. Data files that exceed a million rows of records should run on a computer with at least 4 gigabytes of dedicated RAM. The length of time that is required for indexing data files depends upon the number of columns within the rows. More columns require more time to index.

## Using the Remote EDM Indexer

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 implementing Exact Data Matching”](#) on page 368.

**Table 12-5** 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 <a href="#">“Installing the Remote EDM Indexer”</a> on page 269. See <a href="#">“Installing from the command line (for Linux)”</a> on page 270.
Step 2	Create an Exact Data Profile on the Enforce Server to use with the Remote EDM Indexer.	See <a href="#">“Creating an EDM profile for remote indexing”</a> on page 271.
Step 3	Copy the Exact Data Profile file to the computer where the Remote EDM Indexer resides.	See <a href="#">“Creating an EDM profile for remote indexing”</a> on page 271.
Step 4	Run the Remote EDM Indexer and create the index files.	See <a href="#">“Remote EDM Indexer command options”</a> on page 274.
Step 5	Copy the index files from the remote machine to the Enforce Server.	See <a href="#">“Copying and using generated index files”</a> on page 275.
Step 6	Load the index files into the Enforce Server.	See <a href="#">“Copying and using generated index files”</a> on page 275.
Step 7	Troubleshoot any problems that occur during the indexing process.	See <a href="#">“Troubleshooting index jobs”</a> on page 276.

## Installing the Remote EDM Indexer

The Remote EDM Indexer is installed from the same installation program as the other Symantec Data Loss Prevention components. Copy the `ProtectInstaller_10.5.exe` file to the remote machine where the data that needs to be indexed resides. The Linux version of Symantec Data Loss Prevention

has a text-based command console option in the installation program that can be used.

See [“Installing from the command line \(for Linux\)”](#) on page 270.

---

**Note:** Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before beginning the installation process.

---

To navigate through the installation process:

- Click **Next** to display the next installation screen.
- Click **Back** to return to the previous installation screen.
- Click **Cancel** to terminate the installation process.

**To install the Remote EDM Indexer**

- 1 Go to the directory where you copied the `ProtectInstaller_10.5.exe` (Windows) or `ProtectInstaller_10.5.sh` (Linux) file.

In some circumstances, you may need to change the file permissions to access the file.

- 2 Run the installation program (either `ProtectInstaller_10.5.exe` or `ProtectInstaller_10.5.sh`).

The installer files unpack and the Welcome screen displays.

- 3 Click **Next** and then accept the Symantec Software License Agreement to continue.
- 4 Select **Indexer** from the list of components that appears and click **Next**.
- 5 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, and then click **Next**.
- 6 For Windows, choose a Start Menu folder and then click **Next**.
- 7 The Installing screen appears and displays an installation progress bar. When you are prompted, click **Finish** to complete the installation.

See [“Uninstalling Remote Indexer on a Windows platform”](#) on page 277.

## Installing from the command line (for Linux)

The following procedure describes how to install from the command line for Linux.

### To install a Remote EDM Indexer

- 1 Log on as root and copy the `ProtectInstaller_10.5.sh` file to the `/tmp` directory on the computer.

- 2 Change the directory to `/tmp` by typing:

```
cd /tmp
```

- 3 You may need to change permissions on the file before you can run the file. If so, type:

```
chmod 775 ProtectInstaller_10.5.sh
```

- 4 Once the file permissions have been changed you can run the `ProtectInstaller_10.5.sh` file, by typing:

```
./ProtectInstaller_10.5.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.

- 5 In 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**.
- 6 In 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**.
- 7 In 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.
- 8 When the installation completes, press **Enter** to close the installer.

See [“Uninstalling Remote Indexer on a Linux platform”](#) on page 277.

## Creating an EDM profile 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 [“Copying and using generated index files”](#) on page 275.

See [“About implementing Exact Data Matching”](#) on page 368.

**To create an EDM profile for remote indexing**

- 1** From the Enforce Server administration console, navigate to the **Manage > Data Profiles > Exact Data** screen.
- 2** Click **Add Exact Data Profile**.
- 3** In the **Name** field, enter a name for the profile.
- 4** In the **Data Source** field, select **Use This File Name**, and enter the name of the index file to create.
- 5** In the **Number of Columns** text box, specify the number of columns in the data source to be indexed.
- 6** If the first row of the data source contains the column names, select the option **Read first row as column names**.
- 7** 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.

- 8** In the **Column Separator Char** field, select the type of character that is used in your data source to separate the columns of data.
- 9** 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:

<b>Data Source Field</b>	<b>System Field</b>
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.
- 16 Once you have finished the configuration of the Exact Data Profile, click 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 to the remote machine where you intend to run the Remote EDM Indexer utility.

## Remote EDM Indexer command options

The Indexer runs from the command line. If you are on Linux, change users to the “protect” user before running the Indexer. (The installation program creates the “protect” user.)

The `data`, `profile`, and `result` options are required with the Remote EDM Indexer. However, if the `data` option is not specified, the utility reads stdin by default. Often the data is piped from the SQL Preindexer utility.

[Table 12-6](#) describes the command options for the Remote EDM Indexer.

**Table 12-6** Remote EDM Indexer options

Option	Description
-data	Specifies the file with the data to be indexed. If this option is not specified, the utility reads data from stdin.
-encoding	Specifies the character encoding of the data to index. The default is ISO-8859-1, but data with non-English characters should use UTF-8 or UTF-16. Optional.
-ignore_date	Overrides the expiration date of the Exact Data Profile if the profile has expired. (By default, an Exact Data Profile expires after 30 days.) Optional.
-profile	Specifies the Exact Data Profile to be used. (This profile is the one that is selected by clicking the “download link” on the Exact Data screen in the Enforce Server management console.) Required.
-result	Specifies the directory where the index files are generated. Required.

**Table 12-6** Remote EDM Indexer options (*continued*)

Option	Description
-verbose	Displays a statistical summation of the indexing operation when the index is complete. Optional.

For example, to specify the profile file named `ExportEDMProfile.edm` and place the generated indexes in the `EDMIndexDirectory` directory, type:

```
RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm
-result=C:\EDMIndexDirectory\
```

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.

## Copying and using generated index files

After you create the index files on a remote machine, the files must be copied to the Enforce Server and loaded.

### 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 `\Vontu\Protect\Index` (Windows) or `/var/Vontu/index` (Linux).
- 3 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**.

**6** In the Indexing section, select **Submit Indexing Job on Save**.

**7** Click **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 [“Creating an EDM profile for remote indexing”](#) on page 271.

## Troubleshooting index jobs

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.

The Remote EDM Indexer generally displays a message that indicates whether the indexing operation was successful or not. The result depends on the error threshold that you specify in the profile. Any error percentage under the threshold completes successfully. More detailed information about the indexing operation is available with the verbose option.

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.

See [“Remote EDM Indexer command options”](#) on page 274.

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

- 1** Locate the `Indexer.properties` file at `\Program Files\Vontu\Protect\config\Indexer.properties` (Windows) or `/opt/Vontu/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.”
- 4 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.

## Uninstalling Remote Indexer on a Windows platform

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

- 1 On the computer where the Indexer is installed, locate and run (double-click) the `\Vontu\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.

See “[About the Remote EDM Indexer](#)” on page 268.

## Uninstalling Remote Indexer on a Linux platform

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/Vontu/Uninstall
```

- 2 Run the Uninstall program by typing:

```
./Uninstall -i console
```

- 3 Follow any on-screen instructions.

See [“About the Remote EDM Indexer”](#) on page 268.

## Implementing policy detection

- [Chapter 13. Detecting data loss](#)
- [Chapter 14. Policy authoring](#)
- [Chapter 15. Creating policies from templates](#)
- [Chapter 16. Configuring policies](#)
- [Chapter 17. Administering policies](#)
- [Chapter 18. Detecting content using Exact Data Matching](#)
- [Chapter 19. Detecting content using Index Document Matching](#)
- [Chapter 20. Detecting content using data identifiers](#)
- [Chapter 21. Detecting content using keyword matching](#)
- [Chapter 22. Detecting content using regular expressions](#)
- [Chapter 23. Detecting file properties](#)
- [Chapter 24. Detecting network incidents](#)
- [Chapter 25. Detecting endpoint events](#)

- [Chapter 26. Detecting described identities](#)
- [Chapter 27. Detecting synchronized identities](#)
- [Chapter 28. Detecting profiled identities](#)
- [Chapter 29. Detecting international content](#)
- [Chapter 30. System data identifiers](#)
- [Chapter 31. Policy templates](#)

# Detecting data loss

This chapter includes the following topics:

- [Introduction to policy detection](#)
- [Available detection technologies](#)
- [Introduction to detection rules](#)
- [Implementing policy detection](#)

## Introduction to policy detection

Symantec Data Loss Prevention detects content from virtually any type of message or file, any user, sender, or recipient, wherever your data or endpoints exist. You can detect both the content and the context of data within your enterprise. You define and manage policies from the centralized, Web-based Enforce Server administration console.

See [“About policies”](#) on page 307.

See [“Available detection technologies”](#) on page 283.

See [“Introduction to detection rules”](#) on page 288.

See [“Implementing policies”](#) on page 317.

See [“Implementing policy detection”](#) on page 299.

## About 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 detection engine 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.

See [“Content matching conditions”](#) on page 289.

Content detection is based on the 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 [“Detectable content types”](#) on page 395.

## About file types that can be detected

Symantec Data Loss Prevention recognizes many types of files and attachments: word-processing formats, multimedia files, spreadsheets, presentations, pictures, encapsulation formats, encryption formats, and others.

See [“File property matching conditions”](#) on page 290.

The detection engine does not rely on the file extension to identify the file type. For example, the detection engine recognizes a Microsoft Word file even if a user changes the file extension to .txt. The detection server checks the binary signature of the file to match its type.

See [“Detectable file types”](#) on page 465.

## About network incidents that can be detected

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 [“Network protocol matching condition”](#) on page 291.

## About 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 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 291.

## About 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 content, exact data, and synchronized directory server matching.

For example, you can detect email messages sent by a specific user, or allow email messages sent from a specific group of users.

See [“Groups \(identities\) matching conditions”](#) on page 292.

## About 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.

See [“Supported languages for detection”](#) on page 56.

The detection engine uses Unicode internally. You can build localized policy rules and exceptions using any detection technology in any supported language.

See [“About implementing non-English language detection”](#) on page 529.

## Available detection technologies

Symantec Data Loss Prevention provides several types of detection technologies to detect data loss. Each type of detection technology provides unique capabilities. Often you combine technologies in policies to achieve precise detection results.

See [“Implementing policy detection”](#) on page 299.

**Table 13-1** Available detection technologies

Technology	Description
Exact Data Matching (EDM)	Match structured data (database, CSV). See <a href="#">“About Exact Data Matching”</a> on page 284.
Indexed Document Matching (IDM)	Match unstructured data (documents). See <a href="#">“About Indexed Document Matching”</a> on page 285.
Described Content Matching (DCM)	Match described content, message context, and identity patterns. See <a href="#">“About Described Content Matching”</a> on page 286.
Directory Group Matching (DGM)	Match exact identities from a directory server or database. See <a href="#">“About Directory Group Matching”</a> on page 287.
Custom detection methods	Match unique data by extending detection capabilities. See <a href="#">“About custom detection”</a> on page 287.

## About Exact Data Matching

Exact Data Matching (EDM) detects content you want to protect that is stored in structured or tabular format. For example, you can use EDM to detect confidential customer information from a database. Or, you can use EDM to detect sensitive financial information from a spreadsheet.

To implement EDM, you identify the structured data you want to protect. You index the data source using the Enforce Server administration console. 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. For precise continuous detection, you can schedule indexing on a regular basis so the data is always current. You configure the Content Matches Exact Data From policy detection rule to match individual pieces of the profiled data. For increased accuracy you can configure the rule to match combinations of data fields from a particular record. Once the data source is indexed and the policy is deployed, the detection engine can detect the data in structured or unstructured format.

Consider the following example.

Your company maintains an employee database that contains five columns:

- First Name
- Last Name
- SSN

- Date of Hire
- Salary

Each row in the database contains information for one employee. You export the records to a data source file. Each record is on a separate line. A comma, tab, or pipe character delimits each data item. For example, one row in the data source file contains `Bob, Smith, 123-45-6789, 05/26/99, $42500`. You index the data source file and create an Exact Data Profile. When you configure the profile, you map the data elements (columns) you want to protect. You then configure the EDM policy rule that references the Exact Data Profile. In this example, the rule matches if a message contains the First Name, Last Name, and SSN together. At runtime, the detection engine reports an incident if it detects "Bob, Smith, 123-45-6789" in any inbound message. But, a message containing "Betty, Smith, 123-45-6789" does not match because that record is not in the profile. A message that contains "Bob, Smith, 415-789-0000" also does not match because the number is not the social security number.

See [“About implementing Exact Data Matching”](#) on page 368.

## About Indexed Document Matching

Indexed Document Matching (IDM) matches unstructured data from sensitive, proprietary documents. Example supported document types include Microsoft Word, PowerPoint, PDF, design plans, source code, CAD/CAM images, financial reports, confidential mergers and acquisition documents, and more.

IDM registers and fingerprints discrete sections of extracted data. It normalizes text by removing punctuation and formatting. The normalization process ensures that the presentation of the content does not affect or disrupt detection.

IDM uses a statistical sampling method to store hash sections of a fingerprinted document. Not all text is stored in the Document Profile. This method allows IDM to have high accuracy rates while also letting you easily scale your policies by adding detection servers. You can also whitelist content and exclude it from matching.

When you configure an IDM policy, you establish the percentage of content that must match the Document Profile to trigger an incident. You can use IDM to detect exact content matches of text documents, if all hashed segments are detected in the fingerprint. In this fashion you can detect derivative documents, such as revisions and versions. You can also use IDM to match partial document content and passages, such as chunks of content copied to other documents or messages.

In addition to full and partial document matching, you can also use IDM to detect binary content. This is implemented by creating an MD5 hash of the binary content in addition to the hashes that are created for partial document matching. You can

use this variation of IDM to detect file types that the system cannot crack and extract the text content, such as media files or proprietary file formats.

See [“About implementing Indexed Document Matching”](#) on page 393.

## About Described Content Matching

Symantec Data Loss Prevention provides a range of detection methods that are known collectively as Described Content Matching (DCM). This style of detection matches data with common characteristics, such as keywords, data types, file metadata, protocol signatures, endpoint destinations, and identity patterns.

You can use DCM to detect any data you can describe, both structured and unstructured. DCM delivers a high degree of accuracy and is easy to implement because you do not have to profile the data source. DCM is most useful when it is not possible to collect all the data you want to protect, but you can describe it. Often you combine DCM with other detection methods to achieve precise results.

See [“About achieving precise detection results”](#) on page 301.

**Table 13-2** Available DCM methods

Method	Description
Data identifiers	Match content using precise patterns and data validators. See <a href="#">“About data identifiers”</a> on page 416.
Keywords	Match content using keywords, key phrases, and keyword dictionaries. See <a href="#">“About implementing keyword matching”</a> on page 449.
Regular expressions	Match characters, patterns, and strings using regular expressions. See <a href="#">“About regular expression matching”</a> on page 457.
File properties	Match file type, name, and size. See <a href="#">“About implementing file property matching”</a> on page 463.
Users, senders, recipients	Match identities based on patterns. See <a href="#">“About described identity matching”</a> on page 503.
Network protocols	Match network traffic based on protocol signatures. See <a href="#">“About network protocol matching”</a> on page 487.
Endpoint events	Match endpoint destinations, devices, and protocols. See <a href="#">“About implementing endpoint event detection”</a> on page 491.

## About Directory Group Matching

Directory Group Matching (DGM) detects the exact identity of data users, message senders, and recipients.

Symantec Data Loss Prevention provides two flavors of Directory Group Matching: synchronized and profiled. Synchronized DGM uses a connection to a directory server instance (Microsoft Active Directory) to match identities. Profiled DGM uses a static Exact Data Profile of a directory server or database to match identities.

To implement synchronized DGM, you define one or more User Groups in the Enforce Server administration console and synchronize the groups with your directory server. You then associate the User Groups with the corresponding Sender/User and Recipient detection rules. When you associate a User Group with either of these rules, the rule only applies to that group of users. For example, you can use directory server matching to detect all email messages that are sent from a specific group of users, such as Engineering.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

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 and Recipient detection rules. Profiled DGM leverages Exact Data Matching (EDM) technology to precisely identify and detect identities. For example, you can use a static DGM profile to identify network user activity or to include the user-associated content in analysis. Or, you can exclude certain email addresses from analysis. Or, you might want to prevent certain people from sending confidential information by email.

See [“About implementing profiled Directory Group Matching”](#) on page 523.

## About custom detection

Symantec Data Loss Prevention provides you with several ways to extend detection and match any type of data, content, or files you want.

You can write scripts, expressions, and plugins to customize the capabilities of the detection engine.

**Table 13-3** Available detection customization methods

Method	Description
Modified data identifiers	Modify system-defined data identifiers to suit your needs.  See <a href="#">“About data identifiers”</a> on page 416.

**Table 13-3** Available detection customization methods (*continued*)

Method	Description
Custom data identifiers	Implement your own data identifier patterns and system-defined validators.  See <a href="#">“Implementing custom data identifiers”</a> on page 443.
Custom validators for data identifiers	Use the Symantec Data Loss Prevention Scripting Language to validate custom data types.  See <a href="#">“Implementing custom data identifiers”</a> on page 443.
Custom file type detection	Use the Symantec Data Loss Prevention Scripting Language to detect custom file types.  See <a href="#">“About custom file type detection”</a> on page 479.
Custom endpoint device detection	Detect or allow any endpoint device using regular expressions.  See <a href="#">“About endpoint device detection”</a> on page 492.
Custom network protocol detection	Define custom TCP ports to tap.  See <a href="#">“About network protocol matching”</a> on page 487.
Custom content extraction	Write a plugin to extract custom content for analysis by the detection engine.  See the <i>Symantec Data Loss Prevention Detection Customization Guide</i> .

## Introduction to detection rules

Symantec Data Loss Prevention provides several types of detection rules, each offering unique capabilities.

You implement detection rules in policies. Rules declare one or more conditions to match data. You can also create exception conditions for rules.

See [“About rule exceptions”](#) on page 296.

**Table 13-4** Detection rule and exception types

Rule type	Description
Content	See <a href="#">“Content matching conditions”</a> on page 289.
File property	See <a href="#">“File property matching conditions”</a> on page 290.

**Table 13-4** Detection rule and exception types (*continued*)

Rule type	Description
Network	See <a href="#">“Network protocol matching condition”</a> on page 291.
Endpoint	See <a href="#">“Endpoint matching conditions”</a> on page 291.
Groups (identity)	See <a href="#">“Groups (identities) matching conditions”</a> on page 292.

## Content matching conditions

Symantec Data Loss Prevention provides several rules to detect message content.

See [“Detectable content types”](#) on page 395.

For content detection, you can match on individual message components: header, subject, body, and attachments.

See [“About message components that can be matched”](#) on page 293.

**Table 13-5** Available content matching conditions

Content rule type	Description
Content Matches Regular Expression	Match described content using regular expressions. See <a href="#">“About regular expression matching”</a> on page 457. See <a href="#">“Configuring the Content Matches Regular Expression condition”</a> on page 457. <b>Note:</b> This detection rule is not available as an exception.
Content Matches Exact Data From an Exact Data Profile	Match exact data from a structured data source such as a database or comma-separated value file. See <a href="#">“About implementing Exact Data Matching”</a> on page 368. See <a href="#">“Configuring the Content Matches Exact Data condition”</a> on page 387.
Content Matches Keyword	Match described content using keywords, key phrases, and data dictionaries. See <a href="#">“About implementing keyword matching”</a> on page 449. See <a href="#">“Configuring the Content Matches Keyword condition”</a> on page 452.

**Table 13-5** Available content matching conditions (*continued*)

Content rule type	Description
Content Matches Document Signature From an Indexed Document Profile	Match unstructured data (document content) exactly using fingerprinting.  See <a href="#">“About implementing Indexed Document Matching”</a> on page 393.  See <a href="#">“Configuring the Content Matches Document Signature condition”</a> on page 411.
Content Matches Data Identifier	Match described content using Data Identifier patterns and validators.  See <a href="#">“About data identifiers”</a> on page 416.  See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.

## File property matching conditions

Symantec Data Loss Prevention provides several methods to detect file properties, including file type, file size, and file name.

See [“About implementing file property matching”](#) on page 463.

**Table 13-6** Available file property detection rules

Detection rule type	Description
Message Attachment or File Type Match	Detect specific file formats and attachments.  See <a href="#">“About file type detection”</a> on page 464.  See <a href="#">“Configuring the Message Attachment or File Type Match condition”</a> on page 481.
Message Attachment or File Size Match	Detect file or attachments over or under a specified size.  See <a href="#">“About file size detection”</a> on page 480.  See <a href="#">“Configuring the Message Attachment or File Size Match condition”</a> on page 482.
Message Attachment or File Name Match	Detect files or attachments that have a specific name or match wildcards.  See <a href="#">“About file name detection”</a> on page 480.  See <a href="#">“Configuring the Message Attachment or File Name Match condition”</a> on page 483.

**Table 13-6** Available file property detection rules (*continued*)

Detection rule type	Description
Message/Email Properties and Attributes	<p>Classify Microsoft Exchange email messages based on specific message attributes (MAPI attributes).</p> <p><b>Note:</b> This detection rule is only available for the Data Classification for Enterprise Vault product. See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.</p>
Custom File Type Signature	<p>Detect custom file types based on their binary signature using scripting.</p> <p>See <a href="#">“About custom file type detection”</a> on page 479.</p> <p>See <a href="#">“Enabling custom file type detection”</a> on page 484.</p>

## Network protocol matching condition

Symantec Data Loss Prevention provides a single method to detect network traffic.

See [“About network protocol matching”](#) on page 487.

**Table 13-7** Network protocol detection rule

Detection rule	Description
Protocol and Endpoint Destination	<p>Detect incidents on the network transmitted using a specified protocol.</p> <p>See <a href="#">“About network incidents that can be detected”</a> on page 282.</p> <p>See <a href="#">“Configuring Protocol Monitoring condition parameters”</a> on page 488.</p>

## Endpoint matching conditions

Symantec Data Loss Prevention provides several methods for detecting endpoint events.

See [“About endpoint events that can be detected”](#) on page 282.

**Table 13-8** Endpoint detection rules

Detection rule	Description
Protocol and Endpoint Destination	<p>Match endpoint messages transmitted using a specified transport protocol.</p> <p>Match endpoint events when data is moved or copied to a particular destination.</p> <p>See <a href="#">“About implementing endpoint event detection”</a> on page 491.</p> <p>See <a href="#">“Configuring Endpoint Monitoring condition parameters”</a> on page 493.</p>
Endpoint Device Class or ID	<p>Match endpoint events occurring on specified hardware devices.</p> <p>See <a href="#">“About implementing endpoint event detection”</a> on page 491.</p> <p>See <a href="#">“Configuring the Endpoint Device Class or ID condition”</a> on page 498.</p>
Endpoint Location	<p>Detect endpoint events depending if the endpoint agent is on or off the corporate network.</p> <p>See <a href="#">“About implementing endpoint event detection”</a> on page 491.</p> <p>See <a href="#">“Configuring the Endpoint Location condition”</a> on page 499.</p>

## Groups (identities) matching conditions

Symantec Data Loss Prevention provides several rules for detecting the identity of users and groups, and message senders and recipients.

See [“About identities that can be detected”](#) on page 283.

**Table 13-9** Available group rules for identity matching

Group rule	Description
Sender/User Matches Pattern	<p>Match message senders and users by email address, user ID, IM screen name, and IP address.</p> <p>See <a href="#">“About described identity matching”</a> on page 503.</p> <p>See <a href="#">“Configuring the Sender/User Matches Pattern condition”</a> on page 504.</p>

**Table 13-9** Available group rules for identity matching (*continued*)

Group rule	Description
Recipient Matches Pattern	<p>Match message recipients by email or IP address, or Web domain.</p> <p>See <a href="#">“About described identity matching”</a> on page 503.</p> <p>See <a href="#">“Configuring the Recipient Matches Pattern condition”</a> on page 506.</p>
Sender/User matches User Group based on a Directory Server	<p>Match message senders and users from a synchronized directory server.</p> <p>See <a href="#">“About implementing synchronized Directory Group Matching”</a> on page 511.</p> <p>See <a href="#">“Configuring the Sender/User matches User Group based on a Directory Server condition”</a> on page 519.</p>
Sender/User matches User Group based on a local Directory from an Exact Data Profile	<p>Match message senders and users from a profiled directory server.</p> <p>See <a href="#">“About implementing profiled Directory Group Matching”</a> on page 523.</p> <p>See <a href="#">“Configuring the Recipient Matches User Group based on a Directory Server condition”</a> on page 520.</p>
Recipient matches User Group based on a Directory Server	<p>Match message recipients from a synchronized directory server.</p> <p>See <a href="#">“About implementing synchronized Directory Group Matching”</a> on page 511.</p> <p>See <a href="#">“Configuring the Sender/User Matches Directory From Exact Data Profile condition”</a> on page 525.</p>
Recipient matches User Group based on a local Directory from an Exact Data Profile	<p>Match message recipients from a profiled directory server.</p> <p>See <a href="#">“About implementing profiled Directory Group Matching”</a> on page 523.</p> <p>See <a href="#">“Configuring the Recipient Matches Directory From Exact Data Profile condition”</a> on page 526.</p>

## About message components that can be matched

The system receives 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 content of the message into one or more components (header, subject, body, attachments), or it

leaves the message intact. The system evaluates the message or message components to see if any 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.

You can configure described content conditions to match across all message components. EDM supports the envelope, body, and attachment components. The document content and File Size conditions match on the message body and attachments. The File Type and File Name conditions match on the message attachment only. Protocol, endpoint, and identity conditions match on the entire message. Any condition that the DLP Agent evaluates matches on the entire message, regardless of any individually selected message components. The subject component only applies to SMTP email or NNTP messages, otherwise, the subject component is ignored if selected.

---

**Note:** The subject component matches 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 [“Selecting components to match on”](#) on page 348.

**Table 13-10** Message components to match on

Condition type	Envelope	Subject	Body	Attachment(s)
Described content (DCM) (Keyword, DI, Regex)	match	match	match	match
Exact data (EDM)	match		match	match
Indexed document content (IDM)			match	match
File Size (DCM)			match	match
File Type and File Name (DCM)				match
Protocol (DCM)	match (entire message)			
Endpoint (DCM)	match (entire message)			

**Table 13-10** Message components to match on (*continued*)

Condition type	Envelope	Subject	Body	Attachment(s)
Identity (DCM and DGM)	match (entire message)			
Any evaluated by the DLP Agent	match (entire message)			

## About rule severity

You set the detection rule severity to flag condition matches with a specific 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 687.

When you configure a detection rule, you select a default severity level. 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.

See [“Defining rule severity”](#) on page 345.

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.

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 13-11** 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.

## About rule exceptions

Symantec Data Loss Prevention provides detection and group exceptions to exclude messages, message components, or identities from detection. Detection exceptions are not required, but are often used to refine the scope of detection and group rules.

See [“About using exceptions to narrow detection scope”](#) on page 304.

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 matches 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 declares a detection rule with one condition and a detection exception with one condition. The rule matches all messages containing Word attachments and generates an incident for each match. The exception excludes any messages from ceo@company.com and does not generate an incident if this exception is matched. In this case, an email from ceo@company.com that contains a Word attachment is excepted from matching and does not trigger an incident. The exception excluding all ceo@company.com messages takes precedence over the detection rule.

See [“About detection execution”](#) on page 297.

You can implement all available detection and group rule conditions as exceptions, except those that implement EDM. You can implement IDM as an exception, but the exception excludes specific document types from detection, not the content in the documents. To exclude content in documents, you need to “whitelist” it.

See [“Adding an exception to a policy”](#) on page 349.

See [“CAN-SPAM Act policy template”](#) on page 605.

See [“Excluding \(whitelisting\) content from detection”](#) on page 404.

## About compound match 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. Optionally, you can declare multiple conditions within a single detection or group rule.

See [“About using compound rules for precise detection”](#) on page 305.

A rule with a single condition is a simple rule. A rule with multiple conditions is a compound rule. For compound rules, each condition must match to trigger an incident. Thus, for a single policy that declares one rule with two conditions, if one condition matches but the other does not, the detection engine does not report a match. If both conditions match, the detection engine reports a match, assuming that the rule is set to count all matches.

See [“About detection execution”](#) on page 297.

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 [“About rule exceptions”](#) on page 296.

## About detection execution

You can include any combination of detection and group rules and exceptions in a single policy. Each rule or exception may contain one or more conditions.

See [“About rule exceptions”](#) on page 296.

The system evaluates exceptions first. If any exception is met, the entire message or message component matching the exception is ejected and is no longer available for detection. No incident is reported.

If no exception is met or present in the policy, the engine evaluates the detection and group rules on a per-rule basis. If the policy contains multiple rules of the same type, the system reports an incident if any rule is met. If there are rules of different types, each must match to report an incident.

In programmatic terms, where you have a single policy definition, the connection between conditions in the same rule or exception is AND. The connection between two or more rules or exceptions of the same type is OR. But, if you combine a group rule (or exception) and a detection rule (or exception) in a single policy, the connection between the rules (or exceptions) is AND. In this configuration both rules (or exceptions) must match to trigger an incident.

See [“Implementing policy detection”](#) on page 299.

**Table 13-12**      Detection engine Boolean execution logic

---

**Table 13-12** Detection engine Boolean execution logic (*continued*)

Logic	Method	Type	Cardinality	Condition	Match
IF	Except 1	Detection or Group	Simple	Condition	Matches
				<b>OR</b>	
	Except N	Detection or Group	Compound	Condition 1	Matches
				<b>AND</b>	
			Condition N	Matches	
THEN	No incident is reported.				
ELSE	Rule 1	Detection	Simple	Condition	Matches
				<b>OR</b>	
	Rule N	Detection	Compound	Condition 1	Matches
				<b>AND</b>	
			Condition N	Matches	
THEN	An incident is reported.				
ELSE	Rule 1	Group	Simple	Condition	Matches
				<b>OR</b>	
	Rule N	Group	Compound	Condition 1	Matches
				<b>AND</b>	
			Condition N	Matches	
THEN	An incident is reported.				
ELSE	Rule N	Group	Simple or compound	Condition N	Matches
				<b>AND</b>	
		Detection	Simple or compound	Condition N	Matches
THEN	An incident is reported.				

# Implementing policy detection

Implementing detection that meets your data loss prevention objectives is a process that involves both business and technical considerations. See the following table for an overview of the process.

**Table 13-13**      Implementing policy detection

Action	Description
Develop a data loss prevention strategy.	Assess your business requirements and develop a data loss prevention strategy.  See <a href="#">“About developing a data loss prevention strategy”</a> on page 300.
Implement a few key policies.	When you are ready to begin with the technology, start small. You can use a few simple rules to address a specific objective and go from there.  See <a href="#">“About policy detection development”</a> on page 301.
Use detection technologies and methods appropriately.	You do not have to create policies and detection rules from scratch. Many policy templates and system-defined data identifiers may be able to address your objectives with little or no modification.  Use the appropriate technology and methods to achieve accurate detection results.  See <a href="#">“About using the appropriate detection method”</a> on page 303.  See <a href="#">“About using exceptions to narrow detection scope”</a> on page 304.  See <a href="#">“About using compound rules for precise detection”</a> on page 305.
Test and refine policy detection.	Fine-tune your detection methods as you generate and examine incidents.  See <a href="#">“About common detection problems to avoid”</a> on page 302.  See <a href="#">“About achieving precise detection results”</a> on page 301.
Implement response rules and deploy policies.	Once you have refined policy detection, you can then implement response rules to take action when policy violations occur.  See <a href="#">“About response rule actions”</a> on page 680.

## About developing a data loss prevention strategy

Data loss prevention begins with detection. To prevent data loss, you must be able to detect when your data is at risk of loss. Only then are you in a position to protect it.

To leverage the power of Symantec Data Loss Prevention detection technologies and capabilities, analyze the types of data you want to protect, how you can detect data loss incidents, and how you want to prevent data loss. In essence you translate your enterprise data security goals into efficient data loss prevention policies that include detection rules and conditions that detect your sensitive data, allow for reasonable uses of your data, and take appropriate response measures to protect your data when violations are detected.

There are two general approaches to developing a data loss prevention strategy:

- Information-based – Identify sensitive data and author policies to prevent it from being lost.
- Regulation-based – Review government and industry regulations and author policies to comply with them.

For the information-based approach, 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.

For the regulation-based approach, 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. Determine the detection methods that work best for you, and revise them as necessary based on the results of your testing.

Lastly, when defining your data loss prevention strategy, consider the planned reporting and remediation structure of your organization. Determine whether your organization is structured around particular bodies of sensitive data or, alternatively, around any particular sets of regulations. Then implement your strategy accordingly.

See [“About recommended roles for your organization”](#) on page 79.

See [“About common detection problems to avoid”](#) on page 302.

See [“About policy detection development”](#) on page 301.

## About policy detection development

You do not have to create complex detection rules to get started with detection. You can add a detection server and deploy one or more basic policies that monitor confidential data without blocking or quarantining it.

See [“Adding a detection server”](#) on page 166.

For example, you can create a policy that defines a Keyword Matching detection rule to detect on the word "confidential." Or, you can leverage 65 pre-built policy detection templates. For example, you can use the HIPAA policy detection template, which uses keyword matching to detect medical sensitive information.

See [“Adding a new policy or policy template”](#) on page 337.

Review the incidents that your policy detects. You can refine your detection rule(s) to minimize false positives before implementing more complex detection methods and rules. For example, you can add another rule based on a Data Profile to detect social security numbers, or a rule based on a User Group to limit policy detection to a specific individuals.

See [“About achieving precise detection results ”](#) on page 301.

## About achieving precise detection results

To prevent data loss, it is necessary to accurately detect all types of confidential data wherever that data is stored, copied, or transmitted. Without accurate detection, a data security system may generate numerous false positives as well as false negatives.

A false positive is a message or file detected as a policy violation that is not a violation. A false negative is a file or a message not detected as a policy violation that is a violation. False positives create high costs in time and resources that are required to investigate and resolve apparent incidents. 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.

When configuring detection rules, try to configure the policies to catch as many real incidents as possible without generating a lot of false positives. If a policy has very broad detection rules, it may generate many false positives. On the other hand, if the detection rules for a policy are too specific, the system may not detect all of the sensitive data.

The best way to achieve precise detection results is to add a policy containing one or two detection conditions, see how many (quantity) and the types (quality) of incidents it generates, then adjust the detection rule(s) as needed. If the policy

generates more false positives than you want, make the detection condition(s) more specific by fine-tuning existing conditions, adding additional conditions, and adding exceptions. If the policy does not detect some incidents, make the detection condition(s) less specific.

See [“About common detection problems to avoid”](#) on page 302.

## About common detection problems to avoid

Symantec Data Loss Prevention provides powerful detection technology. With careful consideration and analysis of your data loss prevention requirements, you can implement efficient detection rules. You must ensure that the detection rules and exceptions are useful and do not degrade system performance. In general, a detection policy that matches a large number of messages may generate too many false positives.

When you create detection policies, two common problems to avoid are the following:

- **Policy too broad.**  
If you add a policy that is too general, it generates incidents when no real match has occurred (false positives). For example, a policy uses a pattern rule looking for the letter "e," which matches nearly every message on the network.
- **Policy too narrow.**  
If your policy has tight rules that are too specific about the data they detect, it may miss many of the matches you want to catch. For example, a policy contains an exception for Word documents and a match condition for Word documents.

The goal is to achieve precision results through well thought-out rules that employ the right type and combination of conditions, and exceptions where necessary.

For example, you want to protect customer names. You create a policy that generates an incident for anything that contains a first and last name. But most messages contain a name—in many cases both first and last names. This policy is too broad. Although your policy may catch all cases of customer names being sent outside the network, this policy may return many false positives. For example, this policy might detect email messages that do not divulge protected information. Since few organizations have the capacity to deal with many false positives, it is important to ensure that your policies report real incidents.

The solution to this problem is to develop policies that look for specific data. One method to achieve this goal is to use database conditions rather than conditions based on patterns. For example, a social security number (SSN) consists of nine digits. That means that there are 1 billion possible SSN numbers of which approximately 800 million are valid. If you base a rule on the SSN pattern of any

nine-digit number, the policy may create an incident for any of the 800 million SSN numbers if they appear in a message. But it also creates incidents for other types of nine-digit numbers, such as European phone numbers, or various types of account numbers. You likely are not interested in protecting all 800 million SSNs and all other nine-digit numbers. In this case you need to find a way to protect only the SSNs in your employee and customer databases. The best way to accomplish that goal is to add a rule using a database condition rather than a pattern condition. This approach provides the most accurate results.

See [“About using the appropriate detection method”](#) on page 303.

## About using the appropriate detection method

To minimize false positives, use the appropriate detection technology and method to detect the data you want to protect.

For example, if you want to detect all social security numbers (SSN), use the SSN Data Identifier instead of a regular expression. The Data Identifier, with its many data patterns and validators, is more precise and better performing than a regular expression. Data Identifiers are more efficient than regular expressions for detecting complex data patterns and execute more quickly at runtime. Data Identifiers include intelligence about valid number ranges for different data types. This additional layer of intelligence lets you screen out test data and other triggers of false positive incidents. It also lets you identify data types specific to a broad range of industries, countries, and regions.

If you want to detect only your employees’ social security numbers, use an Exact Data Profile that contains the specific SSNs in your employee database. An EDM profile is more precise than the SSN Data Identifier. Another way to reduce false positives is to search for combinations of data. If the EDM profile includes fields for first name, last name, and social security number, you can configure a policy that looks for content in which social security numbers appear with the related first and last names. Depending on your requirements, such a policy might be more likely to detect significant data loss than a policy that detects on SSN only.

Another example is the Content Matches Exact Data rule, which lets you specify precise combinations of the columns required for a match. With the Data Identifier or a regular expression detection rules, you can find only social security number patterns. With EDM, you can detect not only a specific social security number, but also the corresponding last name of the person who owns it.

Suppose the following fields exist in your database:

- First Name
- Last Name
- SSN

A policy that protects only the First Name and Last Name fields generates a large number of false positives. Similarly, a policy that protects only the SSN field might generate false positives if there are other types of nine-digit numbers in the database. You need to add a policy that links a particular SSN with a particular first name and last name. A policy that protects the first name, last name, and SSN on each record does catch fewer incidents than the other policies mentioned. However, this policy can still generate incidents that result from an employee sending out the first name, last name, and SSN.

To avoid this problem, configure the condition to require two or more instances of first name, last name, and SSN per message. With this approach, you reduce the number of false positives, but you can still miss some real incidents. For example, if Bob sends out Alice's first name, last name, and SSN, it would not be detected.

Directory Group Matching (DGM) detects employee and group-based user attributes that you index from a corporate LDAP (Active Directory) or human resources database. Static DGM leverages the same fingerprinting technology as EDM to protect data based on user activity. Static DGM uses an exact data index to detect policy violations, without directly accessing the directory. To use static DGM you need to create an exact data profile with specific data fields to identify individual users.

See [“About using exceptions to narrow detection scope”](#) on page 304.

See [“About using compound rules for precise detection”](#) on page 305.

## About using exceptions to narrow detection scope

Detection exceptions can be included to exclude common or non-confidential data. They are implemented to help refine the scope of detection.

Suppose the following fields exist in your database:

- First Name
- Last Name
- SSN
- Phone Number
- Account Number

Initially you may want to add a policy that specifies that any email message that contains any two of these fields is an incident. But you may find that the vast majority of reported incidents contain a first name and last name. In this case your rule needs to be more specific. To achieve the best results, you can add an exception for first name and last name combinations.

See [“About rule exceptions”](#) on page 296.

See [“About detection execution”](#) on page 297.

See [Table 16-8](#) on page 350.

## About using compound rules for precise detection

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 pattern rule for the word CONFIDENTIAL. Such a configuration would achieve more precise detection results.

In addition, to resolve the problem of a policy generating too many incidents, you can set the incident maximum. To do so, you can configure each detection server to report a specific number of incidents over a given time period. The default is 10,000 incidents per server over a 24-hour period.

See [“About compound match conditions”](#) on page 297.



# Policy authoring

This chapter includes the following topics:

- [About policies](#)
- [About policy components](#)
- [About system-defined policy templates](#)
- [About solution packs](#)
- [About policy groups](#)
- [About policy deployment](#)
- [About policy authoring privileges](#)
- [About policy template import and export](#)
- [About Data Profiles](#)
- [About User Groups](#)
- [Implementing policies](#)
- [Policy best practices](#)

## About policies

You implement policies to detect and prevent data loss. A 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.

See [“About developing a data loss prevention strategy”](#) on page 300.

The Enforce Server administration console provides a centralized, Web-based interface for authoring policies.

See [“About policy components”](#) on page 309.

**Table 14-1** Policy authoring features

Feature	Description
Intuitive policy building	<p>The policy builder interface supports Boolean logic for detection configuration.</p> <p>You can combine different detection methods and technologies in a single policy.</p> <p>See <a href="#">“About detection execution”</a> on page 297.</p>
Decoupled response rules	<p>The system stores response rules and policies as separate entities.</p> <p>You can manage and update response rules without having to change policies; you can reuse response rules across policies.</p> <p>See <a href="#">“About response rules”</a> on page 680.</p>
Fine-grained policy reporting	<p>The system provides severity levels for policy violations.</p> <p>You can report the overall severity of a policy violation by the highest severity.</p> <p>See <a href="#">“About rule severity”</a> on page 295.</p>
Centralized data and group profiling	<p>The system stores data and group profiles separate from policies.</p> <p>This separation enables you to manage and update profiles without changing policies.</p> <p>See <a href="#">“About Data Profiles”</a> on page 316.</p>
Template-based policy authoring	<p>The system provides 65 pre-built policy templates.</p> <p>You can use these templates to quickly configure and deploy policies.</p> <p>See <a href="#">“About system-defined policy templates”</a> on page 310.</p>
Policy sharing	<p>The system supports policy template import and export.</p> <p>You can share policy templates across environments and systems.</p> <p>See <a href="#">“About policy template import and export”</a> on page 314.</p>
Role-based access control	<p>The system provides role-based access control for various user and administrative functions.</p> <p>You can create roles for policy authoring, policy administration, and response rule authoring.</p> <p>See <a href="#">“About policy authoring privileges”</a> on page 313.</p>

See [“Implementing policies”](#) on page 317.

See [“Introduction to policy detection”](#) on page 281.

## About policy components

A valid policy must declare at least one detection or group rule with at least one match condition. Response rules are optional policy components.

See [“About policies”](#) on page 307.

**Table 14-2** Policy components

Component	Use	Description
Policy group	Required	A policy must be assigned to a single Policy Group. See <a href="#">“About policy groups”</a> on page 311.
Policy name	Required	The policy name must be unique within the Policy Group. See <a href="#">“Manage and add policies”</a> on page 357.
Policy rule	Required	A valid policy must contain at least one rule that declares at least one match condition. See <a href="#">“Introduction to detection rules”</a> on page 288.
Data Profile	May be required	A policy requires a Data Profile if a detection method in the policy requires it. See <a href="#">“About Data Profiles”</a> on page 316.
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 <a href="#">“About User Groups”</a> on page 317.
Policy description	Optional	A policy description helps users identify the purpose of the policy. See <a href="#">“Configuring policies”</a> on page 338.
Response Rule	Optional	A policy can implement one or more response rules to report and remediate incidents. See <a href="#">“About response rules”</a> on page 680.

**Table 14-2** Policy components (*continued*)

Component	Use	Description
Policy exception	Optional	A policy can contain one or more exceptions to exclude data from matching.  See <a href="#">“About rule exceptions”</a> on page 296.
Compound match conditions	Optional	A policy rule or exception can implement multiple match conditions.  See <a href="#">“About compound match conditions”</a> on page 297.

See [“About policy template import and export”](#) on page 314.

## About system-defined policy templates

Symantec Data Loss Prevention provides policy templates to help you quickly deploy data loss 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.

See [“Creating a policy from a template”](#) on page 321.

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 [“About policy template import and export”](#) on page 314.

**Table 14-3** Available policy templates

Policy template type	Description
US Regulatory Enforcement	See <a href="#">“US Regulatory Enforcement policy templates”</a> on page 324.
UK and International Regulatory Enforcement	See <a href="#">“UK and International Regulatory Enforcement policy templates”</a> on page 327.

**Table 14-3** Available policy templates (*continued*)

Policy template type	Description
Customer and Employee Data Protection	See “ <a href="#">Customer and Employee Data Protection policy templates</a> ” on page 327.
Confidential or Classified Data Protection	See “ <a href="#">Confidential or Classified Data Protection policy templates</a> ” on page 329.
Network Security Enforcement	See “ <a href="#">Network Security Enforcement policy templates</a> ” on page 330.
Acceptable Use Enforcement	See “ <a href="#">Acceptable Use Enforcement policy templates</a> ” on page 331.
Imported Templates	See “ <a href="#">About policy template import and export</a> ” on page 314.
Classification for Enterprise Vault	See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> .

## About 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 357.

## About 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.

See [“About solution packs”](#) on page 311.

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.

See [“About solution packs”](#) on page 311.

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, Network 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 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 360.

See [“Creating and modifying policy groups”](#) on page 359.

## About 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.

See [“About policy groups”](#) on page 311.

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).

See [“About role-based access control”](#) on page 77.

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 best practices”](#) on page 318.

## About 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.

See [“About role-based access control”](#) on page 77.

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.

See [“About response rule authoring privileges”](#) on page 690.

**Table 14-4** Policy authoring privileges

Role privilege	Description
Author Policies	<ul style="list-style-type: none"> <li>■ Add, configure, and manage policies.</li> <li>■ Add, configure, and manage policy rules and exceptions.</li> <li>■ Import and export policy templates.</li> <li>■ Modify system-defined data identifiers and create custom data identifiers.</li> <li>■ Add, configure, and manage User Groups.</li> <li>■ Add response rules to policies (but do not create response rules).</li> </ul>
Enforce Server Administration	<ul style="list-style-type: none"> <li>■ Add, configure, and manage policy groups.</li> <li>■ Add, configure, and manage Data Profiles for EDM and IDM.</li> </ul>
Author Response Rules	<ul style="list-style-type: none"> <li>■ Add, configure, and manage response rules (but do not add them to policies).</li> </ul>

## About policy template 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.

See [“Importing policy templates”](#) on page 361.

See [“Exporting policy detection as a template”](#) on page 362.

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.

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.

See [“Importing version 10 data identifier or keyword policies to version 11 systems”](#) on page 362.

**Table 14-5** Components included in policy templates

Policy component	Included in Template
<p>Policy metadata (name, description).</p> <p>The name of the template has to be less than 60 characters or it does not appear in the <b>Imported Templates</b> list.</p>	YES
<p>Described Content Matching (DCM) rules and exceptions.</p> <p>If the template contains only DCM methods, it imports as exported without changes.</p> <p><b>Note:</b> Version 10 policy templates with Data Identifier or Keyword Matching rules or exceptions cannot be imported to version 11 systems. See <a href="#">“Importing version 10 data identifier or keyword policies to version 11 systems”</a> on page 362.</p>	YES
<p>A single EDM detection rule, or a single IDM detection rule or exception.</p> <p>If the template contains multiple EDM or IDM methods, only one is exported.</p> <p>If the template contains an EDM and an IDM method, the system drops the IDM.</p>	YES
<p>User group methods.</p> <p>User group methods are maintained on import only if the user groups exist on the target before import.</p>	NO
<p>Policy groups do not export.</p> <p>On import you can select a local policy group, otherwise the system assigns the policy to the Default Policy group.</p>	NO
<p>Response Rules do not export.</p> <p>You must define and add response rules to policies from the local Enforce Server instance.</p>	NO
<p>Data Profiles do not export.</p> <p>On import you must reference a locally defined Data Profile, otherwise the system drops any methods that require a Data Profile.</p>	NO
<p>Modified and custom data identifiers do not export.</p>	NO
<p>Custom protocols do not export.</p>	NO
<p>Policy state (Active/Suspended) does not export.</p>	NO

# About Data Profiles

Symantec Data Loss Prevention lets you create Data Profiles for precise detection of sensitive data and content.

**Table 14-6** Data Profiles for precise detection

Data Profile type	Description
Exact Data Profile (EDM)	Contains exact data that has been indexed from a structured data source, such as a database, directory server, keyword dictionary, or CSV file.  See <a href="#">“About implementing Exact Data Matching”</a> on page 368.
Indexed Document Profile (IDM)	Contains exact document content that has been indexed and fingerprinted.  See <a href="#">“About implementing Indexed Document Matching”</a> on page 393.

The Indexed Document Profile contains an indexed set of confidential documents, such as financial documents, draft press releases, source code, and others. These documents can exist on a network file share or you can upload them to the Enforce Server. You create the Data Profile to detect when versions of the indexed documents are found or when sections of these documents are exposed.

See [“Implementing Indexed Document Matching”](#) on page 402.

The Exact Data Profile contains an index of structured data that you export from a database or CSV file. For example, an employee database might contain columns for First Name, Last Name, SSN, Date of Hire, and Salary. Each row in that database would contain one value in each column; for example, Bob Smith 000-00-000 05/26/99 \$42500. When you export the database to a file to create the Exact Data Profile, each row appears as a separate line. Delimiters (comma, tab, or pipe characters) separate each data item in a row. A row in the Exact Data Profile appears as follows: Bob, Smith, 000-00-000, 05/26/99, \$42500. When you create an Exact Data Profile, you protect the data in each row of the database. For example, your policy specifies that if First Name, Last Name, and SSN are found together, it is a match and generates an incident. If a message contains Joe, Smith, 000-00-0000, it is not a match because the first names do not match. If a message contains Bob, Smith, 000-00-0000, however, it is a match that generates an incident.

See [“Implementing Exact Data Matching”](#) on page 368.

At runtime, EDM and IDM rules are evaluated on the server against the profile. If the policy is deployed to an endpoint, the DLP Agent sends the message to the detection server for evaluation (two-tier detection).

## About 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 [“About Directory Group Matching”](#) on page 287.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

See [“Creating and managing directory server connections”](#) on page 513.

See [“Creating or modifying a User Group”](#) on page 517.

## Implementing policies

Policies define the content, event context, and identities you want to detect. Policies may also define response actions if a policy is violated.

See [“About policies”](#) on page 307.

Successful policy creation is a process that requires careful analysis and proper configuration to achieve optimum results.

**Table 14-7** Policy implementation process

Action	Description
Familiarize yourself with the different types of detection technologies and methods that Symantec Data Loss Prevention provides.	See <a href="#">“Available detection technologies”</a> on page 283. See <a href="#">“Introduction to detection rules”</a> on page 288. See <a href="#">“About policy authoring privileges”</a> on page 313.

**Table 14-7** Policy implementation process (*continued*)

Action	Description
Develop a policy detection strategy that defines the type of data you want to protect from data loss.	See <a href="#">“About developing a data loss prevention strategy”</a> on page 300.
Review the policy templates that ship with Symantec Data Loss Prevention, and any templates that you import manually or by solution pack.	See <a href="#">“About system-defined policy templates”</a> on page 310. See <a href="#">“About solution packs”</a> on page 311.
Create policy groups to control how your policies are accessed, edited, and deployed.	See <a href="#">“About policy groups”</a> on page 311. See <a href="#">“About policy deployment”</a> on page 312.
To detect exact data or content or similar unstructured data, create one or more Data Profiles.	See <a href="#">“About Data Profiles”</a> on page 316.
To detect exact identities from a synchronized directory server (Active Directory), configure one or more User Groups.	See <a href="#">“About User Groups”</a> on page 317.
Configure conditions for detection and group rules and exceptions.	See <a href="#">“Creating a policy from a template”</a> on page 321.
Test and refine your policies.	See <a href="#">“About achieving precise detection results”</a> on page 301.
Add response rules to the policy to take action when the policy is violated.	See <a href="#">“About response rules”</a> on page 680.
Manage the policies in your enterprise.	See <a href="#">“Manage and add policies”</a> on page 357.

## Policy best practices

When implementing policies, consider the following:

- Use the system-provided policy templates as starting points for implementing policies.  
See [“About system-defined policy templates”](#) on page 310.
- Well-authored policies accurately detect protected data and content with minimal false positives. Start small with detection. Enable one or two policy templates or a few simple conditions, such as keyword matching. Review the incidents the policy detects. Tune the results before you implement response rules to take action.  
See [“Implementing policy detection”](#) on page 299.
- Consider the roles you need to implement policies. Policy authoring privileges grant access to policy configuration, including rules and exceptions. Enforce Server administrator privileges grant access to Data Profile definition and management. Response rule authoring privileges are separate privileges from policy authoring.  
See [“About recommended roles for your organization”](#) on page 79.
- 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 refine the policies and confirm that they capture the expected incidents, rename the policy group and grant the appropriate roles access to it.  
See [“About policy groups”](#) on page 311.
- Use policy groups to manage legacy policies, as well as policies you want to import or plan to export.  
See [“About removing policies and policy groups”](#) on page 364.



# 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 [“About system-defined policy templates”](#) on page 310.

See [“About policy template import and export”](#) on page 314.

**Table 15-1** Create a policy from a template

Action	Description
Add a policy from a template.	See <a href="#">“Adding a new policy or policy template”</a> on page 337.
Choose the template you want to use.	<p>At the <b>Manage &gt; Policies &gt; Policy List &gt; New Policy - Template List</b> screen the system lists all policy templates.</p> <p>System-provided template categories:</p> <ul style="list-style-type: none"> <li>■ See <a href="#">“US Regulatory Enforcement policy templates”</a> on page 324.</li> <li>■ See <a href="#">“UK and International Regulatory Enforcement policy templates”</a> on page 327.</li> <li>■ See <a href="#">“Customer and Employee Data Protection policy templates”</a> on page 327.</li> <li>■ See <a href="#">“Confidential or Classified Data Protection policy templates”</a> on page 329.</li> <li>■ See <a href="#">“Network Security Enforcement policy templates”</a> on page 330.</li> <li>■ See <a href="#">“Acceptable Use Enforcement policy templates”</a> on page 331.</li> </ul> <p><b>Imported Templates</b> appear individually after import:</p> <ul style="list-style-type: none"> <li>■ See <a href="#">“Importing policy templates”</a> on page 361.</li> </ul> <p><b>Note:</b> See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for information about Classification policy templates.</p>
Click <b>Next</b> to configure the policy.	<p>For example, select the <b>Webmail</b> policy template and click <b>Next</b>.</p> <p>See <a href="#">“Configuring policies”</a> on page 338.</p>

**Table 15-1** Create a policy from a template (*continued*)

Action	Description
<p>Choose a Data Profile (if prompted).</p>	<p>If the template relies on one or more Data Profiles, the system prompts you to select each:</p> <ul style="list-style-type: none"> <li>■ Exact Data Profile See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</li> <li>■ Indexed Document Profile See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.</li> </ul> <p>If you do not have a Data Profile, you can either:</p> <ul style="list-style-type: none"> <li>■ Cancel the policy definition process, define the profile, and resume creating the policy from the template.</li> <li>■ Click <b>Next</b> to configure the policy. On creation of the policy, the system drops any rules or exceptions that rely on the Data Profile.</li> </ul> <p><b>Note:</b> You should use a profile if a template calls for it.</p>
<p>Edit the policy name or description (optional).</p>	<p>If you intend to modify a system-defined template, you may want to change the name so you can distinguish it from the original.</p> <p>See <a href="#">“Configuring policies”</a> on page 338.</p> <p><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.</p>
<p>Select a policy group (if necessary).</p>	<p>If you have defined a policy group, select it from the <b>Policy Group</b> list.</p> <p>See <a href="#">“Creating and modifying policy groups”</a> on page 359.</p> <p>If you have not defined a policy group, the system deploys the policy to the <b>Default Policy Group</b>.</p>
<p>Edit the policy rules or exceptions (if necessary).</p>	<p>The <b>Configure Policy</b> screen displays the rules and exceptions (if any) provided by the policy.</p> <p>You can modify, add, and remove policy rules and exceptions to meet your requirements.</p> <p>See <a href="#">“Configuring policy rules”</a> on page 342.</p> <p>See <a href="#">“Configuring policy exceptions”</a> on page 351.</p>

**Table 15-1** Create a policy from a template (*continued*)

Action	Description
Save the policy and export it (optional).	<p>Click <b>Save</b> to save the policy.</p> <p>You can export policy detection as a template for sharing or archiving.</p> <p>See <a href="#">“Exporting policy detection as a template”</a> on page 362.</p> <p>For example, if you changed the configuration of a system-defined policy template, you may want to export it for sharing across environments.</p>
Test and tune the policy (recommended).	<p>Test and tune the policy using data the policy should and should not detect.</p> <p>Review the incidents that the policy generates. Refine the policy rules and exceptions as necessary to reduce false positives and false negatives.</p> <p>See <a href="#">“Implementing policy detection”</a> on page 299.</p>
Add response rules (optional).	<p>Add response rules to the policy to report and remediate violations.</p> <p>See <a href="#">“Implementing policy response rules”</a> on page 691.</p> <p><b>Note:</b> Response rules are not included in policy templates.</p>

## US Regulatory Enforcement policy templates

Symantec Data Loss Prevention provides several policy templates supporting US Regulatory Enforcement guidelines.

See [“Creating a policy from a template”](#) on page 321.

**Table 15-2** US Regulatory Enforcement policy templates

Policy template	Description
CAN-SPAM Act	<p>Establishes requirements for sending commercial email.</p> <p>See <a href="#">“CAN-SPAM Act policy template”</a> on page 605.</p>
Defense Message System (DMS) GENSER Classification	<p>Detects information classified as confidential.</p> <p>See <a href="#">“Defense Message System (DMS) GENSER Classification policy template”</a> on page 613.</p>

**Table 15-2** US Regulatory Enforcement policy templates (*continued*)

Policy template	Description
Export Administration Regulations (EAR)	Enforces the U.S. Department of Commerce Export Administration Regulations (EAR).  See <a href="#">“Export Administration Regulations (EAR) policy template”</a> on page 618.
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 <a href="#">“FACTA 2003 (Red Flag Rules) policy template”</a> on page 619.
Gramm-Leach-Bliley	This policy limits sharing of consumer information by financial institutions.  See <a href="#">“Gramm-Leach-Bliley policy template”</a> on page 625.
HIPAA and HITECH (including PHI)	This policy enforces the US Health Insurance Portability and Accountability Act (HIPAA).  See <a href="#">“HIPAA and HITECH (including PHI) policy template”</a> on page 627.
International Traffic in Arms Regulations (ITAR)	This policy enforces the US Department of State ITAR provisions.  See <a href="#">“International Traffic in Arms Regulations (ITAR) policy template”</a> on page 633.
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 <a href="#">“NASD Rule 2711 and NYSE Rules 351 and 472 policy template”</a> on page 637.
NASD Rule 3010 and NYSE Rule 342	This policy monitors brokers-dealers communications.  See <a href="#">“NASD Rule 3010 and NYSE Rule 342 policy template”</a> on page 638.

**Table 15-2** US Regulatory Enforcement policy templates (*continued*)

Policy template	Description
NERC Security Guidelines for Electric Utilities	<p>This policy detects the information that is outlined in the North American Electric Reliability Council (NERC) security guidelines for the electricity sector.</p> <p>See <a href="#">“NERC Security Guidelines for Electric Utilities policy template”</a> on page 640.</p>
Office of Foreign Assets Control (OFAC)	<p>This template detects communications involving targeted OFAC groups.</p> <p>See <a href="#">“Office of Foreign Assets Control (OFAC) policy template”</a> on page 644.</p>
OMB Memo 06-16 and FIPS 199 Regulations	<p>This template detects information that is classified as confidential.</p> <p>See <a href="#">“OMB Memo 06-16 and FIPS 199 Regulations policy template”</a> on page 646.</p>
Payment Card Industry Data Security Standard	<p>This template detects Visa and MasterCard credit card number data.</p> <p>See <a href="#">“Payment Card Industry (PCI) Data Security Standard policy template”</a> on page 648.</p>
Sarbanes-Oxley	<p>This template detects sensitive financial data.</p> <p>See <a href="#">“Sarbanes-Oxley policy template”</a> on page 656.</p>
SEC Fair Disclosure Regulation	<p>This template detects data disclosure of material financial information.</p> <p>See <a href="#">“SEC Fair Disclosure Regulation policy template”</a> on page 658.</p>
State Data Privacy	<p>This template detects breaches of state-mandated confidentiality.</p> <p>See <a href="#">“State Data Privacy policy template”</a> on page 662.</p>
US Intelligence Control Markings (CAPCO) and DCID 1/7	<p>This template detects authorized terms to identify classified information in the US Federal Intelligence community.</p> <p>See <a href="#">“US Intelligence Control Markings (CAPCO) and DCID 1/7 policy template”</a> on page 669.</p>

# 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 321.

**Table 15-3** UK and International Regulatory Enforcement policy templates

Policy template	Description
Caldicott Report	This policy protects UK patient information. See <a href="#">“Caldicott Report policy template”</a> on page 603.
UK Data Protection Act 1998	This policy protects personal identifiable information. See <a href="#">“Data Protection Act 1998 (UK) policy template”</a> on page 611.
EU Data Protection Directives	This policy detects personal data specific to the EU directives. See <a href="#">“Data Protection Directives (EU) policy template”</a> on page 612.
Human Rights Act 1998	This policy enforces Article 8 of the act for UK citizens. See <a href="#">“Human Rights Act 1998 policy template”</a> on page 631.
PIPEDA	This policy detects Canadian citizen customer data. See <a href="#">“PIPEDA policy template”</a> on page 649.

# Customer and Employee Data Protection policy templates

Symantec Data Loss Prevention provides several policy templates for Customer and Employee Data Protection.

See [“Creating a policy from a template”](#) on page 321.

**Table 15-4** Customer and Employee Data Protection policy templates

Policy template	Description
Canadian Social Insurance Numbers	<p>This policy detects patterns indicating Canadian social insurance numbers.</p> <p>See <a href="#">“Canadian Social Insurance Numbers policy template”</a> on page 605.</p>
Credit Card Numbers	<p>This policy detects patterns indicating credit card numbers.</p> <p>See <a href="#">“Credit Card Numbers policy template”</a> on page 609.</p>
Customer Data Protection	<p>This policy detects customer data.</p> <p>See <a href="#">“Customer Data Protection policy template”</a> on page 609.</p>
Employee Data Protection	<p>This policy detects employee data.</p> <p>See <a href="#">“Employee Data Protection policy template”</a> on page 616.</p>
Individual Taxpayer Identification Numbers (ITIN)	<p>This policy detects IRS-issued tax processing numbers.</p> <p>See <a href="#">“Individual Taxpayer Identification Numbers (ITIN) policy template”</a> on page 633.</p>
SWIFT Codes	<p>This policy detects codes banks use to transfer money across international borders.</p> <p>See <a href="#">“SWIFT Codes policy template”</a> on page 666.</p>
UK Drivers License Numbers	<p>This policy detects UK Drivers License Numbers.</p> <p>See <a href="#">“UK Drivers License Numbers policy template”</a> on page 667.</p>
UK Electoral Roll Numbers	<p>This policy detects UK Electoral Roll Numbers.</p> <p>See <a href="#">“UK Electoral Roll Numbers policy template”</a> on page 667.</p>
UK National Insurance Numbers	<p>This policy detects UK National Insurance Numbers.</p> <p>See <a href="#">“UK National Insurance Numbers policy template”</a> on page 668.</p>
UK National Health Service Number	<p>This policy detects personal identification numbers issued by the NHS.</p> <p>See <a href="#">“UK National Health Service (NHS) Number policy template”</a> on page 668.</p>

**Table 15-4** Customer and Employee Data Protection policy templates  
*(continued)*

Policy template	Description
UK Passport Numbers	This policy detects valid UK passports. See <a href="#">“UK Passport Numbers policy template”</a> on page 669.
UK Tax ID Numbers	This policy detects UK Tax ID Numbers. See <a href="#">“UK Tax ID Numbers policy template”</a> on page 669.
US Social Security Numbers	This policy detects patterns indicating social security numbers. See <a href="#">“US Social Security Numbers policy template”</a> on page 671.

## Confidential or Classified Data Protection policy templates

Symantec Data Loss Prevention provides several policy templates for Confidential or Classified Data Protection.

See [“Creating a policy from a template”](#) on page 321.

**Table 15-5** Confidential or Classified Data Protection policy templates

Policy template	Description
Confidential Documents	This policy detects company-confidential documents. See <a href="#">“Confidential Documents policy template”</a> on page 608.
Design Documents	This policy detects various types of design documents. See <a href="#">“Design Documents policy template”</a> on page 615.
Encrypted Data	This policy detects the use of encryption by a variety of methods. See <a href="#">“Encrypted Data policy template”</a> on page 617.
Financial Information	This policy detects financial data and information. See <a href="#">“Financial Information policy template”</a> on page 623.

**Table 15-5** Confidential or Classified Data Protection policy templates  
*(continued)*

Policy template	Description
Merger and Acquisition Agreements	This policy detects information and communications about upcoming merger and acquisition activity.  See <a href="#">“Merger and Acquisition Agreements policy template”</a> on page 635.
Price Information	This policy detects specific SKU or pricing information.  See <a href="#">“Price Information policy template”</a> on page 651.
Project Data	This policy detects discussions of sensitive projects.  See <a href="#">“Project Data policy template”</a> on page 652.
Proprietary Media Files	This policy detects various types of video and audio files.  See <a href="#">“Proprietary Media Files policy template”</a> on page 652.
Publishing Documents	This policy detects various types of publishing documents.  See <a href="#">“Publishing Documents policy template”</a> on page 653.
Resumes	This policy detects active job searches.  See <a href="#">“Resumes policy template”</a> on page 655.
Source Code	This policy detects various types of source code.  See <a href="#">“Source Code policy template”</a> on page 661.
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 <a href="#">“Symantec DLP Awareness and Avoidance policy template”</a> on page 666.

## 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 321.

**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 <a href="#">“Common Spyware Upload Sites policy template”</a> on page 607.
Network Diagrams	This policy detects computer network diagrams.  See <a href="#">“Network Diagrams policy template”</a> on page 642.
Network Security	This policy detects evidence of hacking tools and attack planning.  See <a href="#">“Network Security policy template”</a> on page 643.
Password Files	This policy detects password file formats.  See <a href="#">“Password Files policy template”</a> on page 647.

## Acceptable Use Enforcement policy templates

Symantec Data Loss Prevention provides several policy templates for allowing acceptable uses of information.

See [“Creating a policy from a template”](#) on page 321.

**Table 15-7** Acceptable Use Enforcement policy templates

Policy template	Description
Competitor Communications	This policy detects forbidden communications with competitors.  See <a href="#">“Competitor Communications policy template”</a> on page 607.
Forbidden Websites	This policy detects access to specified Web sites.  See <a href="#">“Forbidden Websites policy template”</a> on page 624.
Gambling	This policy detects any reference to gambling.  See <a href="#">“Gambling policy template”</a> on page 624.
Illegal Drugs	This policy detects conversations about illegal drugs and controlled substances.  See <a href="#">“Illegal Drugs policy template”</a> on page 632.

**Table 15-7** Acceptable Use Enforcement policy templates (*continued*)

Policy template	Description
Media Files	This policy detects various types of video and audio files. See “ <a href="#">Media Files policy template</a> ” on page 634.
Offensive Language	This policy detects the use of offensive language. See “ <a href="#">Offensive Language policy template</a> ” on page 643.
Racist Language	This policy detects the use of racist language. See “ <a href="#">Racist Language policy template</a> ” on page 654.
Restricted Files	This policy detects various file types that are generally inappropriate to send out of the company. See “ <a href="#">Restricted Files policy template</a> ” on page 654.
Restricted Recipients	This policy detects communications with specified recipients. See “ <a href="#">Restricted Recipients policy template</a> ” on page 655.
Sexually Explicit Language	This policy detects vulgar, sexually explicit, and pornographic content. See “ <a href="#">Sexually Explicit Language policy template</a> ” on page 660.
Violence and Weapons	This policy detects violent language and discussions about weapons. See “ <a href="#">Violence and Weapons policy template</a> ” on page 671.
Webmail	This policy detects the use of a variety of Webmail services. See “ <a href="#">Webmail policy template</a> ” on page 671.
Yahoo Message Board Activity	This policy detects Yahoo message board activity. See “ <a href="#">Yahoo Message Board Activity policy template</a> ” on page 672.
Yahoo and MSN Messengers on Port 80	This policy detects Yahoo IM and MSN Messenger activity. See “ <a href="#">Yahoo and MSN Messengers on Port 80 policy template</a> ” on page 674.

# 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.

See [“About Exact Data Matching”](#) on page 284.

## To use an Exact Data Profile

- 1 Select an **Exact Data Profile** from the list of available profiles.
- 2 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 321.

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 [“About implementing Exact Data Matching”](#) on page 368.

---

**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 the 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.

---

**Table 15-8** Policy templates that implement Exact Data Matching (EDM)

Policy template	Description
Caldicott Report	See <a href="#">“Caldicott Report policy template”</a> on page 603.
Customer Data Protection	See <a href="#">“Customer Data Protection policy template”</a> on page 609.
Data Protection Act 1988	See <a href="#">“Data Protection Act 1998 (UK) policy template”</a> on page 611.
Employee Data Protection	See <a href="#">“Employee Data Protection policy template”</a> on page 616.
EU Data Protection Directives	See <a href="#">“Data Protection Directives (EU) policy template”</a> on page 612.
Export Administration Regulations (EAR)	See <a href="#">“Export Administration Regulations (EAR) policy template”</a> on page 618.

**Table 15-8** Policy templates that implement Exact Data Matching (EDM)  
*(continued)*

Policy template	Description
FACTA 2003 (Red Flag Rules)	See <a href="#">“FACTA 2003 (Red Flag Rules) policy template”</a> on page 619.
Gramm-Leach-Bliley	See <a href="#">“Gramm-Leach-Bliley policy template”</a> on page 625.
HIPAA and HITECK (including PHI)	See <a href="#">“HIPAA and HITECH (including PHI) policy template”</a> on page 627.
Human Rights Act 1998	See <a href="#">“Human Rights Act 1998 policy template”</a> on page 631.
International Traffic in Arms Regulations (ITAR)	See <a href="#">“International Traffic in Arms Regulations (ITAR) policy template”</a> on page 633.
Payment Card Industry Data Security Standard	See <a href="#">“Payment Card Industry (PCI) Data Security Standard policy template”</a> on page 648.
PIPEDA	See <a href="#">“PIPEDA policy template”</a> on page 649.
Price Information	See <a href="#">“Price Information policy template”</a> on page 651.
Resumes	See <a href="#">“Resumes policy template”</a> on page 655.
State Data Privacy	See <a href="#">“SEC Fair Disclosure Regulation policy template”</a> on page 658.

## 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 [“About Indexed Document Matching”](#) on page 285.

### To use a Document Profile

- 1 Select the **Document Profile** from the list of available profiles.
- 2 Click **Next** to create the policy from the template.

See [“Creating a policy from a template”](#) on page 321.

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 implementing Indexed Document Matching”](#) on page 393.

**Table 15-9** Policy templates that implement Indexed Document Matching (IDM)

Policy template	Description
CAN-SPAM Act (IDM exception)	See <a href="#">“CAN-SPAM Act policy template”</a> on page 605.
NASD Rule 2711 and NYSE Rules 351 and 472	See <a href="#">“NASD Rule 2711 and NYSE Rules 351 and 472 policy template”</a> on page 637.
NERC Security Guidelines for Electric Utilities	See <a href="#">“NERC Security Guidelines for Electric Utilities policy template”</a> on page 640.
Sarbanes-Oxley	See <a href="#">“Sarbanes-Oxley policy template”</a> on page 656.
SEC Fair Disclosure Regulation	See <a href="#">“SEC Fair Disclosure Regulation policy template”</a> on page 658.
Confidential Documents	See <a href="#">“Confidential Documents policy template”</a> on page 608.
Design Documents	See <a href="#">“Design Documents policy template”</a> on page 615.
Financial Information	See <a href="#">“Financial Information policy template”</a> on page 623.
Project Data	See <a href="#">“Project Data policy template”</a> on page 652.
Proprietary Media Files	See <a href="#">“Proprietary Media Files policy template”</a> on page 652.
Publishing Documents	See <a href="#">“Publishing Documents policy template”</a> on page 653.
Source Code	See <a href="#">“Source Code policy template”</a> on page 661.
Network Diagrams	See <a href="#">“Network Diagrams policy template”</a> on page 642.



# 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](#)

## Adding a new policy or policy template

As a policy author you can define a new policy from scratch or from a template.

See [“Implementing policies”](#) on page 317.

**To add a new policy or a policy template**

- 1 Click **Add Policy** at the **Manage > Policies > Policy List** screen.  
 See “[Manage and add policies](#)” on page 357.
- 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 “[About policy components](#)” on page 309.  
 Select **Add a policy from a template** to add a policy from a template.  
 See “[About system-defined policy templates](#)” on page 310.
- 3 Click **Next** to configure the policy or the policy template.  
 See “[Configuring policies](#)” on page 338.  
 See “[Creating a policy from a template](#)” on page 321.  
 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** Configuring policies

Action	Description
Define a new policy, or edit an existing policy.	<p>Add a new blank policy.            See “<a href="#">Adding a new policy or policy template</a>” on page 337.</p> <p>Create a policy from a template.            See “<a href="#">Creating a policy from a template</a>” on page 321.</p> <p>Select an existing policy at the <b>Manage &gt; Policies &gt; Policy List</b> screen to edit it.            See “<a href="#">Manage and add policies</a>” on page 357.</p>
Enter a policy <b>Name</b> and <b>Description</b> .	<p>The policy name must be unique in the policy group you deploy the policy to.</p> <p>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.</p>

**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 <a href="#">“Creating and modifying policy groups”</a> on page 359.
Set the <b>Status</b> for the policy.	You can enable (default setting) or disable a policy. A disabled policy is deployed but does not detect incidents.  See <a href="#">“Manage and add policies”</a> on page 357.
Add a rule to the policy, or edit an existing rule.	Click <b>Add Rule</b> to add a rule.  See <a href="#">“Adding a rule to a policy”</a> on page 340.  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 <a href="#">“Configuring policy rules”</a> on page 342.
Optionally, add one or more policy exceptions, or edit an existing exception.	Click <b>Add Exception</b> to add it.  See <a href="#">“Adding an exception to a policy”</a> on page 349.  Select an existing exception to edit it.
Configure any exception(s).	See <a href="#">“Configuring policy exceptions”</a> on page 351.
Save the policy configuration.	Click <b>Save</b> to save the policy configuration to the Enforce Server database.  See <a href="#">“About policy components”</a> on page 309.
Export the policy as a template.	Optionally, you can export the policy rules and exceptions as a template.  See <a href="#">“Exporting policy detection as a template”</a> on page 362.
Add one or more response rules to the policy.	You configure response rules independent of policies.  See <a href="#">“Configuring response rules”</a> on page 697.  See <a href="#">“Adding a response rule to a policy”</a> on page 363.

---

**Note:** The **Policy Actions** setting only applies to Classification policies. See the *Enterprise Vault Data Classification Services Implementation Guide* for more information.

---

## 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 [“About detection execution”](#) on page 297.

**Table 16-2** Adding policy rules

Rule	Prerequisite	Description
<b>Content</b>		
Content Matches Regular Expression		See <a href="#">“About regular expression matching”</a> on page 457.
Content Matches Exact Data	Exact Data Profile	See <a href="#">“About implementing Exact Data Matching”</a> on page 368. See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.
Content Matches Keyword		See <a href="#">“About implementing keyword matching”</a> on page 449.
Content Matches Document Signature	Indexed Document Profile	See <a href="#">“About implementing Indexed Document Matching”</a> on page 393. See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.
Content Matches Data Identifier	Data Identifier	See <a href="#">“About data identifiers”</a> on page 416. See <a href="#">“Selecting system data identifier breadth”</a> on page 436.
<b>File Properties</b>		
Message Attachment or File Type Match		See <a href="#">“About file type detection”</a> on page 464.

**Table 16-2** Adding policy rules (*continued*)

Rule	Prerequisite	Description
Message Attachment or File Size Match		See <a href="#">“About file size detection”</a> on page 480.
Message Attachment or File Name Match		See <a href="#">“About file name detection”</a> on page 480.
Message/Email Properties and Attributes	Enterprise Vault integration	See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.
Custom File Type Signature	Rule enabled Custom script	See <a href="#">“About custom file type detection”</a> on page 479.
<b>Protocol and Endpoint</b>		
Protocol Monitoring	Custom protocols (if any)	See <a href="#">“About network protocol matching”</a> on page 487.
Endpoint Monitoring		See <a href="#">“About endpoint protocol, destination, and application detection”</a> on page 492.
Endpoint Device Class or ID	Custom device(s)	See <a href="#">“About endpoint device detection”</a> on page 492.
Endpoint Location		See <a href="#">“About endpoint location detection”</a> on page 493.
<b>Groups (Identities)</b>		
Sender/User Matches Pattern Recipient Matches Pattern		See <a href="#">“About described identity matching”</a> on page 503.
Sender/User Matches User Group based on a Directory Server Group Recipient Matches User Group based on a Directory Server Group	User Group	See <a href="#">“About implementing synchronized Directory Group Matching”</a> on page 511. See <a href="#">“Creating or modifying a User Group”</a> on page 517.

**Table 16-2** Adding policy rules (*continued*)

Rule	Prerequisite	Description
Sender/User Matches User Group based on a local Directory	Exact Data Profile	See <a href="#">“About implementing profiled Directory Group Matching”</a> on page 523.
Recipient Matches User Group based on a local Directory		See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.

**To add one or more rules to a policy**

- 1 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 [“Introduction to detection rules”](#) on page 288.
- 2 Select the detection or the group rule you want to implement from the list of rules.  
 See [Table 16-2](#) on page 340.
- 3 Select the prerequisite component, if required.  
 If the policy rule requires a **Data Profile**, **Data Identifier**, or **User Group** select it from the list.
- 4 Click **Next** to configure the policy rule.  
 See [“Configuring policy rules”](#) on page 342.

---

**Note:** Select the **Exception** tab to add a policy exception. See [“Adding an exception to a policy”](#) on page 349.

---

## 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 16-3](#) on page 343.

**Table 16-3** Configuring policy rule conditions

Rule	Description
<b>Content</b>	
Content Matches Regular Expression	See <a href="#">“Configuring the Content Matches Regular Expression condition”</a> on page 457.
Content Matches Exact Data	See <a href="#">“Configuring the Content Matches Exact Data condition”</a> on page 387.
Content Matches Keyword	See <a href="#">“Configuring the Content Matches Keyword condition”</a> on page 452.
Content Matches Document Signature	See <a href="#">“Configuring the Content Matches Document Signature condition”</a> on page 411.
Content Matches Data Identifier	See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.
<b>File Properties</b>	
Message Attachment or File Type Match	See <a href="#">“Configuring the Message Attachment or File Type Match condition”</a> on page 481.
Message Attachment or File Size Match	See <a href="#">“Configuring the Message Attachment or File Size Match condition”</a> on page 482.
Message Attachment or File Name Match	See <a href="#">“Configuring the Message Attachment or File Name Match condition”</a> on page 483.
Email/MAPI Attributes	See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.
Custom File Type Signature	See <a href="#">“Configuring the Custom File Type Signature condition”</a> on page 485.
<b>Protocol and Endpoint</b>	
Network Monitoring	See <a href="#">“Configuring Protocol Monitoring condition parameters”</a> on page 488.
Endpoint Monitoring	See <a href="#">“Configuring Endpoint Monitoring condition parameters”</a> on page 493.
Endpoint Device Class or ID	See <a href="#">“Configuring the Endpoint Device Class or ID condition”</a> on page 498.
Endpoint Location	See <a href="#">“Configuring the Endpoint Location condition”</a> on page 499.

**Table 16-3** Configuring policy rule conditions (*continued*)

Rule	Description
<b>Group (identity)</b>	
Sender/User Matches Pattern	See <a href="#">“Configuring the Sender/User Matches Pattern condition”</a> on page 504.
Recipient Matches Pattern	See <a href="#">“Configuring the Recipient Matches Pattern condition”</a> on page 506.
Sender/User Matches User Group Based on a Directory Server	See <a href="#">“Configuring the Sender/User matches User Group based on a Directory Server condition”</a> on page 519.
Recipient Matches User Group Based on Exact Data Profile	See <a href="#">“Configuring the Recipient Matches User Group based on a Directory Server condition”</a> on page 520.
Sender/User Matches User Group Based on a Directory Server	See <a href="#">“Configuring the Sender/User Matches Directory From Exact Data Profile condition”</a> on page 525.
Recipient Matches User Group Based on Exact Data Profile	See <a href="#">“Configuring the Recipient Matches Directory From Exact Data Profile condition”</a> on page 526.

**Table 16-4** Configuring policy rules

Step	Action	Description
Step 1	Add a rule to a policy, or modify a rule.	See <a href="#">“Adding a rule to a policy”</a> on page 340.  To modify an existing rule, select the rule in the policy builder interface at the <b>Configure Policy – Edit Rule</b> 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.
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 <a href="#">“Defining rule severity”</a> on page 345.
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 <a href="#">Table 16-3</a> on page 343.

**Table 16-4** Configuring policy rules (*continued*)

Step	Action	Description
Step 5	Configure match counting (if required).	If the rule calls for it, configure how you want to count matches.  See <a href="#">“Configuring match counting”</a> on page 346.
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 <a href="#">“Selecting components to match on”</a> on page 348.
Step 7	Add and configure one or more additional match conditions (optional).	To define a compound rule, <b>Add</b> another match condition from the <b>Also Match</b> list.  Configure the additional condition according to its type (Step 3).  See <a href="#">“Configuring compound match conditions”</a> on page 354.  <b>Note:</b> All conditions in a single rule must match to trigger an incident.  See <a href="#">“About detection execution”</a> on page 297.
Step 8	Save the policy configuration.	When you are done configuring 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 <a href="#">“Manage and add policies”</a> on page 357.

## 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 [“About rule severity”](#) on page 295.

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 711.

**To define policy rule severity**

- 1 Configure a policy rule.  
 See “[Configuring policy rules](#)” on page 342.
- 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.
- 4 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.
- 6 To remove a defined severity level, click the **X** icon beside the severity definition.

## 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 347.

**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.

**Table 16-5** Configuring match counting (*continued*)

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	<p>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.</p> <p>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.</p>
	Only report incidents with at least _ matches	<p>You can change the default one incident per match count by specifying the minimum number of matches required to report an incident.</p> <p>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.</p> <p><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.</p>

**Table 16-6** Conditions that support match counting

Condition	Description
Content Matches Regular Expression	<p>See <a href="#">“About regular expression matching”</a> on page 457.</p> <p>See <a href="#">“Configuring the Content Matches Regular Expression condition”</a> on page 457.</p>

**Table 16-6** Conditions that support match counting (*continued*)

Condition	Description
Content Matches Keyword	See <a href="#">“About implementing keyword matching”</a> on page 449. See <a href="#">“Configuring the Content Matches Keyword condition”</a> on page 452.
Content Matches Document Signature (IDM)	See <a href="#">“About implementing Indexed Document Matching”</a> on page 393. See <a href="#">“Configuring the Content Matches Document Signature condition”</a> on page 411.
Content Matches Data Identifier	See <a href="#">“About data identifiers”</a> on page 416. See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.
Recipient Matches Pattern	See <a href="#">“About described identity matching”</a> on page 503. See <a href="#">“Configuring the Recipient Matches Pattern condition”</a> on page 506.

**Note:** Exact Data Matching supports match counting, but it is configured at the **Advanced Server Settings** screen. See [“About configuring exact data match counting”](#) on page 371.

## 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 [“About message components that can be matched”](#) on page 293.

**Table 16-7** Match on components

Component	Description
Envelope	<p>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.</p> <p>If the condition does not support matching on the <b>Envelope</b> component, this option is grayed out.</p> <p>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.</p>

**Table 16-7** Match on components (*continued*)

Component	Description
Subject	<p>Certain detection conditions match on the <b>Subject</b> component for some types of messages.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p> <p>For the detection conditions that support subject component matching, you can match on the <b>Subject</b> for the following types of messages:</p> <ul style="list-style-type: none"> <li>■ SMTP (email) messages from Network Monitor or Network Prevent (Email).</li> <li>■ NNTP messages from Network Monitor.</li> <li>■ Exchange email messages delivered by the Classification Server.</li> </ul> <p>See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.</p> <p>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.</p>
Body	<p>If the condition matches on the <b>Body</b> message component, select it to match on the text or content of the message.</p>
Attachment(s)	<p>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.</p>

## Adding an exception to a policy

At the **Manage > Policies > Policy List > Configure Policy – Add Exception** screen you add one or more exceptions to a policy. If the policy matches an exception, the detection engine does not trigger an incident.

See [“About rule exceptions”](#) on page 296.

You can add one or more detection or group exceptions to a policy. Policy exceptions are executed before policy rules.

See [“About detection execution”](#) on page 297.

---

**Note:** You can create exceptions for all policy rules, except those that implement Exact Data Matching.

---

**Table 16-8** Selecting a policy exception

Exception	Prerequisites	Description
<b>Content</b>		
Content Matches Regular Expression		See <a href="#">“About regular expression matching”</a> on page 457.
Content Matches Keyword		See <a href="#">“About implementing keyword matching”</a> on page 449.
Content Matches Document Signature	Indexed Document Profile	See <a href="#">“About implementing Indexed Document Matching”</a> on page 393. See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.
Content Matches Data Identifier	Data Identifier	See <a href="#">“About data identifiers”</a> on page 416. See <a href="#">“Selecting system data identifier breadth”</a> on page 436.
<b>File Properties</b>		
Message Attachment or File Type Match		See <a href="#">“About file type detection”</a> on page 464.
Message Attachment or File Size Match		See <a href="#">“About file size detection”</a> on page 480.
Message Attachment or File Name Match		See <a href="#">“About file name detection”</a> on page 480.
Message/Email Properties and Attributes	Enterprise Vault integration	See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.
Custom File Type Signature	Exception enabled Custom script	See <a href="#">“About custom file type detection”</a> on page 479.
<b>Protocol and Endpoint</b>		
Network Protocol		See <a href="#">“About network protocol matching”</a> on page 487.
Endpoint Protocol, Destination, Application		See <a href="#">“About endpoint protocol, destination, and application detection”</a> on page 492.

**Table 16-8** Selecting a policy exception (*continued*)

Exception	Prerequisites	Description
Endpoint Device Class or ID		See <a href="#">“About endpoint device detection”</a> on page 492.
Endpoint Location		See <a href="#">“About endpoint location detection”</a> on page 493.
<b>Group (identity)</b>		
Sender/User Matches Pattern Recipient Matches Pattern		See <a href="#">“About described identity matching”</a> on page 503.
Sender/User Matches User Group based on a Directory Server Recipient Matches User Group based on a Directory Server	User Group	See <a href="#">“About implementing synchronized Directory Group Matching”</a> on page 511. See <a href="#">“Creating or modifying a User Group”</a> on page 517.

### To add an exception to a policy

- 1 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 350.

- 3 If necessary, choose the profile, data identifier, or user group.
- 4 Click **Next** to configure the exception.

See [“Configuring policy exceptions”](#) on page 351.

## 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 16-9](#) on page 352.

If an exception condition matches, the system discards the matched component from the system. This component is no longer available for evaluation.

See [“About rule exceptions”](#) on page 296.

**Table 16-9** Configuring policy exception conditions

Exception	Description
<b>Content</b>	
Content Matches Regular Expression	See <a href="#">“Configuring the Content Matches Regular Expression condition”</a> on page 457.
Content Matches Keyword	See <a href="#">“Configuring the Content Matches Keyword condition”</a> on page 452.
Content Matches Document Signature	See <a href="#">“Configuring the Content Matches Document Signature condition”</a> on page 411.
Content Matches Data Identifier	See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.
<b>File Properties</b>	
Message Attachment or File Type Match	See <a href="#">“Configuring the Message Attachment or File Type Match condition”</a> on page 481.
Message Attachment or File Size Match	See <a href="#">“Configuring the Message Attachment or File Size Match condition”</a> on page 482.
Message Attachment or File Name Match	See <a href="#">“Configuring the Message Attachment or File Name Match condition”</a> on page 483.
Email/MAPI Attributes	See the <i>Enterprise Vault Data Classification Services Implementation Guide</i> for more information.
Custom File Type Signature	See <a href="#">“Configuring the Custom File Type Signature condition”</a> on page 485.
<b>Protocol and Endpoint</b>	
Network Protocol	See <a href="#">“Configuring Protocol Monitoring condition parameters”</a> on page 488.
Endpoint Protocol or Destination	See <a href="#">“Configuring Endpoint Monitoring condition parameters”</a> on page 493.
Endpoint Device Class or ID	See <a href="#">“Configuring the Endpoint Device Class or ID condition”</a> on page 498.

**Table 16-9** Configuring policy exception conditions (*continued*)

Exception	Description
Endpoint Location	See <a href="#">“Configuring the Endpoint Location condition”</a> on page 499.
<b>Group (identity)</b>	
Sender/User Matches Pattern	See <a href="#">“Configuring the Sender/User Matches Pattern condition”</a> on page 504.
Recipient Matches Pattern	See <a href="#">“Configuring the Recipient Matches Pattern condition”</a> on page 506.
Sender/User Matches User Group on a Directory Server	See <a href="#">“Configuring the Sender/User matches User Group based on a Directory Server condition”</a> on page 519.
Recipient Matches User Group on a Directory Server	See <a href="#">“Configuring the Sender/User Matches Directory From Exact Data Profile condition”</a> on page 525.

**Table 16-10** Configure policy exceptions

Step	Action	Description
Step 1	Add a new policy exception, or edit an existing exception.	See <a href="#">“Adding an exception to a policy”</a> on page 349. 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. <b>Note:</b> 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 <a href="#">“About message components that can be matched”</a> on page 293. Select one of the <b>Apply Exception to</b> options: <ul style="list-style-type: none"> <li>■ <b>Entire Message</b> This option applies the exception to the entire message.</li> <li>■ <b>Matched Components Only</b> This option applies the exception to each message component you select from the <b>Match On</b> options in the <b>Conditions</b> section of the exception.</li> </ul>

**Table 16-10**      Configure policy exceptions (*continued*)

Step	Action	Description
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 <a href="#">Table 16-9</a> on page 352.
Step 5	Add one or more additional conditions to the exception (optional).	You can add conditions until the exception is structured as desired.  See <a href="#">“Configuring compound match conditions”</a> on page 354.  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.
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 <a href="#">“Manage and add policies”</a> on page 357.

## Configuring compound match conditions

You can create compound match conditions for policy rules and exceptions.

See [“Configuring compound match conditions”](#) on page 354.

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 [“About detection execution”](#) on page 297.

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 [“About using compound rules for precise detection”](#) on page 305.

**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 <b>Configure Policy – Edit Rule</b> 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 condition.	Select the additional match condition from the <b>Also Match</b> list.  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.  <a href="#">See “Adding a rule to a policy”</a> on page 340.  <a href="#">See “Adding an exception to a policy”</a> on page 349.
Step 4	Add the additional condition.	Click <b>Add</b> to add the additional match condition to the policy rule or exception.  Once added, you can collapse and expand each condition in a rule or exception.
Step 5	Configure the additional condition.	<a href="#">See “Configuring policy rules”</a> on page 342.  <a href="#">See “Configuring policy exceptions”</a> on page 351.
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.  <b>Same Component</b> – 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.  <a href="#">See “About cross-component matching for data identifiers”</a> on page 425.
Step 6	Repeat this process to additional match conditions to the rule or exception.	You can add as many conditions to a rule or exception as you need.  All conditions in a single rule or exception must match to trigger an incident, or to trigger the exception.

**Table 16-11**      Configure a compound policy rule or exception (*continued*)

Step	Action	Description
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.

# Administering policies

This chapter includes the following topics:

- [Manage and add policies](#)
- [Creating and modifying policy groups](#)
- [Manage and add policy groups](#)
- [Importing policy templates](#)
- [Exporting policy detection as a template](#)
- [Importing version 10 data identifier or keyword policies to version 11 systems](#)
- [Adding a response rule to a policy](#)
- [About removing policies and policy groups](#)

## Manage and add policies

You implement policies to detect and report data loss. The **Manage > Policies > Policy List** screen is the home page for adding and managing policies.

See [“Implementing policies”](#) on page 317.

**Table 17-1** Policy List screen actions

Action	Description
Add Policy	Click <b>Add Policy</b> to create a new policy. See <a href="#">“Adding a new policy or policy template”</a> on page 337.
Modify Policy	Click anywhere in the policy row to modify an existing policy. See <a href="#">“Configuring policies”</a> on page 338.

**Table 17-1** Policy List screen actions (*continued*)

Action	Description
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 <b>column header</b> 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. <b>Note:</b> You cannot remove a policy that has active incidents. See <a href="#">“About removing policies and policy groups”</a> on page 364.
Export and Import Policy Templates	See <a href="#">“Importing policy templates”</a> on page 361. See <a href="#">“Exporting policy detection as a template”</a> on page 362.

**Table 17-2** Policy List screen display fields

Column	Description
Name	View and sort by the name of the policy. See <a href="#">“About policies”</a> on page 307.
Description	View the description of the policy. See <a href="#">“About system-defined policy templates”</a> on page 310.
Policy Group	View and sort by the policy group to which the policy is deployed. See <a href="#">“About policy groups”</a> on page 311.
Last Modified	View and sort by the date the policy was last updated. See <a href="#">“About policy authoring privileges”</a> on page 313.
Misconfigured Policy	The policy icon is a yellow caution sign. See <a href="#">“About policy components”</a> on page 309. See <a href="#">“Response rule best practices”</a> on page 692.
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.

# Creating and modifying policy groups

At the **System > Servers > Policy Groups** screen you configure a new policy group or modify an existing one.

See [“About policy groups”](#) on page 311.

## To configure a policy group

- 1 Add a new policy group, or modify an existing one.

See [“Manage and add policy groups”](#) on page 360.

- 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.

- 4 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 857.

- 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 338.

See [“About policy deployment”](#) on page 312.

## 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.

**Table 17-3** Policy Groups screen actions

Action	Description
Add Policy Group	Click <b>Add Policy Group</b> to define a new policy group. See <a href="#">“About policy groups”</a> on page 311.
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 <a href="#">“Creating and modifying policy groups”</a> on page 359.
Remove Policy Group	Click the red <b>X</b> icon to the far right of the row to delete that policy group from the system. 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 <a href="#">“About removing policies and policy groups”</a> on page 364.
View policies in a group	To view the policies deployed to an existing policy group, navigate to the <b>System &gt; Servers &gt; Policy Groups &gt; Configure Policy Group</b> screen. See <a href="#">“Creating and modifying policy groups”</a> on page 359.

**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 <a href="#">“About policy deployment”</a> on page 312.
Last Modified	The date the policy group was last modified.

## 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 [“About policy template import and export”](#) on page 314.

### To import one or more policy templates to the Enforce Server

- 1 Place one or more policy templates XML file(s) in the `\Vontu\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.
- 3 Log on to the Enforce Server Administration Console with policy authoring privileges.
- 4 Navigate to **Manage > Policies > Policy List** and click **Add Policy**.
- 5 Choose the option **Add a policy from a template** and click **Next**.
- 6 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“Importing version 10 data identifier or keyword policies to version 11 systems”](#) on page 362.

## 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 [“About policy template import and export”](#) on page 314.

### To export a policy as a template

- 1 Log on to the Enforce Server administration console with administrator privileges.
- 2 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.
- 4 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 361.

See [“Importing version 10 data identifier or keyword policies to version 11 systems”](#) on page 362.

## Importing version 10 data identifier or keyword policies to version 11 systems

Symantec Data Loss Prevention version 11 implements significant enhancements to the data identifier and keyword matching detection methods. These changes are not backward-compatible. You cannot import a policy template from a version 10 system to a version 11 system if the template contains a keyword match or data identifier condition.

See [“About policy template import and export”](#) on page 314.

If you have a version 10 policy that contains only keyword or data identifier conditions, you have to rebuild the entire policy on a version 11 system. If you have a version 10 policy that contains keyword or data identifier conditions and other types of conditions, you can use the following workaround.

### To import version 10 data identifier or keyword policy templates to version 11 systems

- 1 On a v10 system, export the policy as is.  
Name it appropriately, such as **Original**.
- 2 Using the version 10 policy builder interface, remove any keyword and data identifier conditions from the policy.  
Rename the policy to **Modified**.
- 3 Export the **Modified** policy as a template from the version 10 system.  
See [“Exporting policy detection as a template”](#) on page 362.
- 4 Import the **Modified** policy template to a version 11 Enforce Server.  
See [“Importing policy templates”](#) on page 361.
- 5 Rebuild the keyword or data identifier conditions you removed from the policy.  
See [“Configuring policies”](#) on page 338.

## Adding a response rule to a policy

You can add one or more response rules to a policy to take action when that policy is violated.

See [“About response rules”](#) on page 680.

### To add a response rule to a policy

- 1 Log on to the Enforce Server administration console with policy authoring privileges.  
See [“About policy authoring privileges”](#) on page 313.
- 2 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 policy response rules”](#) on page 691.
- 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.
- 7 Verify that the policy status is green after adding the response rule to the policy.

See [“Manage and add policies”](#) on page 357.

---

**Note:** If the policy status is a yellow caution sign, the policy is misconfigured. The system does not support certain response rule action – policy detection rule or exception pairings.

See [Table 63-2](#) on page 1062.

---

See [“Response rule best practices”](#) on page 692.

## About removing policies and policy groups

Consider the following guidelines before you delete a policy or a policy group from the Enforce Server.

**Table 17-5** Guidelines for removing policies and policy groups

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 <a href="#">“Manage and add policies”</a> on page 357.  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 <a href="#">“About policy template import and export”</a> on page 314.

**Table 17-5** Guidelines for removing policies and policy groups (*continued*)

Action	Description	Guideline
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.	<p>Before you delete a policy group, remove any policies from that group by either deleting them or assigning them to different policy groups.</p> <p>See <a href="#">“Manage and add policy groups”</a> on page 360.</p> <p>If you want to remove a policy group, create a maintenance policy group and move the policies you want to remove to the maintenance group.</p> <p>See <a href="#">“Creating and modifying policy groups”</a> on page 359.</p>

See [“About policies”](#) on page 307.

See [“About policy groups”](#) on page 311.

See [“Policy best practices”](#) on page 318.



# Detecting content using Exact Data Matching

This chapter includes the following topics:

- [About implementing Exact Data Matching](#)
- [Implementing Exact Data Matching](#)
- [About data owner exception](#)
- [About field mappings](#)
- [About index scheduling](#)
- [About configuring exact data match counting](#)
- [Manage and add Exact Data Profiles](#)
- [Creating the exact data source file](#)
- [Migrating legacy data owner exception configurations](#)
- [Preparing the exact data source file for indexing](#)
- [Uploading exact data source files to the Enforce Server](#)
- [Creating and modifying Exact Data Profiles](#)
- [Mapping Exact Data Profile fields](#)
- [Scheduling Exact Data Profile indexing](#)
- [Configuring the Content Matches Exact Data condition](#)
- [EDM best practices](#)

## About implementing Exact Data Matching

To detect data exactly, Symantec Data Loss Prevention requires a special indexed version of the data. An index is a secure file (or set of files). It 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, so it is secure.

See [“About Exact Data Matching”](#) on page 284.

Indexes consist of one or more secure, binary .rdx files, each with space to fit into random access memory (RAM) on the detection server(s). For a large data source file, Symantec Data Loss Prevention may break the data into several .rdx files. In production, 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 .rdx files, identifying matches.

By default, Symantec Data Loss Prevention stores index files in

`C:\Vontu\Protect\index` (on Windows) or in `/var/Vontu/index` (on Linux) on the Enforce Server and on all detection servers. When the policy is active, Symantec Data Loss Prevention deploys the index to the detection server and the detection server loads the index into RAM.

See [“Implementing Exact Data Matching”](#) on page 368.

## Implementing Exact Data Matching

To implement EDM, you create the Exact Data Profile, index the data source, and define one or more EDM detection rules to match the profiled data exactly.

**Table 18-1** Implementing Exact Data Matching

Step	Action	Description
1	Create the data source file.	<p>Export the source data from the database (or other data repository) to a tabular text file.</p> <p>See <a href="#">“About data owner exception”</a> on page 370.</p> <p>If you want to except data owners from matching, you need to include specific data items in the data source file.</p> <p>See <a href="#">“About implementing profiled Directory Group Matching”</a> on page 523.</p> <p>If you want to match identities for profiled Directory Group Matching (DGM), you need to include specific data items in the data source files.</p> <p>See <a href="#">“About profiling keyword dictionaries”</a> on page 455.</p>
2	Prepare the data source file for indexing.	<p>Remove irregularities from the data source file.</p> <p>See <a href="#">“Preparing the exact data source file for indexing”</a> on page 376.</p>
3	Upload the data source file to the Enforce Server.	<p>You can copy or upload the data source file to the Enforce Server, or access it remotely.</p> <p>See <a href="#">“Uploading exact data source files to the Enforce Server”</a> on page 378.</p>
4	Create an Exact Data Profile.	<p>The Exact Data Profile specifies the data source, the indexing parameters, and the indexing schedule.</p> <p>See <a href="#">“Creating and modifying Exact Data Profiles”</a> on page 379.</p>
5	Map the data fields.	<p>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.</p> <p>See <a href="#">“About field mappings”</a> on page 370.</p> <p>See <a href="#">“Mapping Exact Data Profile fields”</a> on page 384.</p>

**Table 18-1** Implementing Exact Data Matching (*continued*)

Step	Action	Description
6	Index the data source, or schedule indexing.	See <a href="#">“About index scheduling”</a> on page 371. See <a href="#">“Scheduling Exact Data Profile indexing”</a> on page 386.
7	Configure and tune one or more EDM detection conditions.	See <a href="#">“Configuring the Content Matches Exact Data condition”</a> on page 387. See <a href="#">“About configuring exact data match counting”</a> on page 371.

See [“EDM best practices”](#) on page 390.

## About data owner exception

The data owner exception (DOE) feature enables data owners to send or receive their own data the system would otherwise prevent from delivery or receipt.

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

Once you have configured the Exact Data Profile that includes either of these data elements, you can flag either field as the data owner. At runtime if the sender or recipient of the data is the owner, the condition does not trigger a match. The result is that the data is delivered or received.

See [“Configuring the Content Matches Exact Data condition”](#) on page 387.

If you previously implemented DOE manually using configuration files, you must reconfigure these exceptions to run on the latest Enforce Server.

See [“Migrating legacy data owner exception configurations”](#) on page 375.

## About field mappings

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. You use the **Field Mappings** section of the **Add Exact Data Profile** screen to specify mappings between fields in your data source. You can also use this screen to specify fields that Symantec Data Loss Prevention recognizes in its

policy templates. The **Field Mappings** section also gives you advanced options for specifying custom fields.

Consider the following example use of field mappings. Your company wants to protect employee data, including employee social security numbers. You create a 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. Prepare your data source and then create an exact data profile. Specify that the social security number field in the data source maps to the "Social Security Number" system field of the policy template.

See ["Mapping Exact Data Profile fields"](#) on page 384.

## About index scheduling

When you configure an Exact Data Profile, you can set a schedule for indexing the data source.

Before you set up a schedule, consider the following:

- 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.

See ["Implementing Exact Data Matching"](#) on page 368.

## About configuring exact data match counting

By adjusting the EDM.MatchCountVariant setting for the detection server, you can configure how EDM matches are counted.

See ["Advanced server settings"](#) on page 174.

As an example, consider a database profile with the following three records:

- Kathy, Stevens, 123-45-6789, 1111-1111-1111-1111
- Kathy, Stevens, 123-45-6789, 2222-2222-2222-2222
- Kathy, Stevens, 123-45-6789, 3333-3333-3333-3333

If the policy rule is set up to match any 3 of 4 and someone sends a message with the following line:

- Kathy, Stevens, 123-45-6789

The matches are counted as follows:

- EDM.MatchCountVariant=1: 3 (number of database profile records matched)
- EDM.MatchCountVariant=2: 1 (number of unique token sets matched)
- EDM.MatchCountVariant=3: 1 (number of inclusive token sets matched)

If someone sends a message with the following 2 lines:

- Kathy, Stevens, 123-45-6789, 1111-1111-1111-1111
- Kathy, Stevens, 123-45-6789

The matches will be counted as follows:

- EDM.MatchCountVariant=1: 3 (number of database profile records matched)
- EDM.MatchCountVariant=2: 2 (number of unique token sets matched)
- EDM.MatchCountVariant=3: 1 (number of inclusive token sets matched, the first token set includes the second one).

See [“Implementing Exact Data Matching”](#) on page 368.

## Manage and add Exact Data Profiles

The **Manage > Data Profiles > Exact Data** screen lists all Exact Data Profiles configured in the system. An Exact Data Profile is required to implement Exact Data Matching (EDM) policies.

See [“About Data Profiles”](#) on page 316.

From the **Exact Data** screen you can manage existing profiles and add new ones.

See [“About implementing Exact Data Matching”](#) on page 368.

**Table 18-2** Exact Data screen actions

Action	Description
Add EDM profile	Click <b>Add Exact Data Profile</b> to define a new Exact Data Profile. See <a href="#">“Implementing Exact Data Matching”</a> on page 368.

**Table 18-2** Exact Data screen actions (*continued*)

Action	Description
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 <a href="#">“Creating and modifying Exact Data Profiles”</a> on page 379.
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 <b>download profile</b> 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.
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 18-3** Exact Data screen details

Column	Description
Exact Data Profile	The name of the exact data profile.
Last Active Version	The version of the exact data profile and the name of the detection server that runs the profile.

**Table 18-3** Exact Data screen details (*continued*)

Column	Description
Status	<p>The current status of the exact data profile, which can be any of the following:</p> <ul style="list-style-type: none"> <li>■ Next scheduled indexing (if it is not currently indexing)</li> <li>■ Sending an index to a detection server</li> <li>■ Indexing</li> <li>■ Deploying to servers</li> </ul> <hr/> <p>In addition, the current status of the indexing process for each detection server, which can be any of the following:</p> <ul style="list-style-type: none"> <li>■ Completed, including a completion date</li> <li>■ Pending index completion (waiting for the Enforce Server to finish indexing the exact data source file)</li> <li>■ Replicating indexing</li> <li>■ Creating index (internally)</li> <li>■ Building caches</li> </ul>
Error messages	<p>The <b>Exact Data</b> screen displays any error messages in red.</p> <p>For example, if the Exact Data Profile is corrupt or does not exist, the system displays an error message.</p>

See “[Configuring the Content Matches Exact Data condition](#)” on page 387.

## Creating the exact data source file

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.

**Table 18-4** Create the exact data source file

Step	Description
1	<p>Export the data you want to protect from a database or other tabular data format, such as an Excel spreadsheet, to a 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.</p> <p>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.</p> <p>The data source file cannot exceed 2.1 billion cells. The size of a data source is otherwise limited only by the available disk space of the Enforce Server host. If you plan to upload the data source 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.</p>
2	<p>Include required data fields for specific EDM implementations:</p> <ul style="list-style-type: none"> <li>■ Data Owner Exception See <a href="#">“About data owner exception”</a> on page 370. See <a href="#">“Migrating legacy data owner exception configurations”</a> on page 375.</li> <li>■ Directory Group Matching See <a href="#">“Creating the Exact Data Profile for static DGM”</a> on page 524.</li> <li>■ Keyword dictionaries See <a href="#">“About profiling keyword dictionaries”</a> on page 455.</li> </ul>
3	<p>Prepare the data source file for indexing.</p> <p>See <a href="#">“Preparing the exact data source file for indexing”</a> on page 376.</p>

## Migrating legacy data owner exception configurations

In previous releases of Symantec Data Loss Prevention, the data owner exception feature was implemented using configuration files. If you implemented data owner exception using configuration files, you need to migrate these exceptions to the current Enforce Server release. In addition, you need to remove any previous data owner exception configuration files from the system.

See [“About data owner exception”](#) on page 370.

### To migrate legacy Data Owner Exceptions configurations

- 1 Remove or comment out any legacy data owner exception entries found in the following configuration file:

```
\\Vontu\protect\config\ownerexception.properties
```

- 2 Use the Enforce Server administration console to map the data owner exception fields when you create the Exact Data Profile.  
See [“Creating and modifying Exact Data Profiles”](#) on page 379.
- 3 Manually configure the legacy data owner exceptions in one or more policies.  
See [“Configuring the Content Matches Exact Data condition”](#) on page 387.

## 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 efficient EDM indexing

- 1 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 reasonably distinct values. For example, credit card numbers, driver’s license numbers, or account numbers (as opposed to first and last names, which are relatively generic).
  - Verify that you have delimited the data source using commas, tabs, or pipes (|). If the data source uses commas as delimiters, remove any commas that do not serve as delimiters. For example, if a value in the address column is 346 Guerrero St., Apt. 2, delete the comma after Guerrero St.

---

**Note:** The pound sign (#), equals sign (=), plus sign (+), semicolon (;) and colon (:) characters are also treated as separators.

---

- 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 than five digits, as these can cause false positives in production.
- 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 (for example, a comma) as an internal delimiter in any such numbers; for example: 123-45-6789, or 123 45 6789, or 123456789, but not 123,45,6789.
- Eliminate duplicate records, which can cause duplicate matches in production.
- Consider whether to break up the data values that include a space. Some data values, such as San Francisco and New York, almost always appear with a space. You can leave such values in a single field. (Note that Symantec Data Loss Prevention detects multiple-word values in input content only if they appear in tabular data, such as in an Excel file.) Other data values, such as the name Joe Brown, may appear in input content with the middle name or initial; for example: Joe R Brown, Joe R. Brown, or Joe Robert Brown. If the value Joe Brown appears in a single field in your data source, Symantec Data Loss Prevention detects only the literal string Joe Brown. It does not detect other variants of the name. To ensure that Symantec Data Loss Prevention detects name variants, divide the name into two fields: a first-name field and a last-name field. You may also want to remove any relatively unimportant text that is separated by a space. For example, for a data value of Mary Jo, you may want to remove Jo entirely.
- Eliminate duplicate records, which can cause duplicate incidents in production.
- Do not index common values. EDM works best with values that are unique. You need to 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 be useful as an EDM value. For example, suppose you want to look for "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.

- 2 Once you have prepared the exact data source file, proceed with the next step in the EDM process: load 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 378.

## 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.

Listed here are the three 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.

### To make the data source available to the Enforce Server

- 1 If you have a large data source file (over 50 MB), copy it to the "datafiles" directory on the host where Enforce is installed.
  - On Windows this directory is located at `Vontu_home\Protect\datafiles` (for example, `C:\Vontu\Protect\datafiles`).
  - On Linux this directory is located at `/var/Vontu/datafiles`.

This option is convenient because it makes the data file available by reference by a drop-down list during configuration of the **Exact Data Profile**. 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.

---

**Note:** Ensure that the Enforce user (usually called "protect") has **modify** permissions (on Windows) or **rw** permissions (on Linux) for all files in the "datafiles" directory.

---

- 2 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 **Exact Data Profile**, you can specify the file path or browse to the directory and upload the data source file.

---

**Note:** 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 first option.

---

- 3 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 the **Remote EDM Indexer Utility**.

See [“About the Remote EDM Indexer”](#) on page 268.

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 machine 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 Indexer.

See [“Using the Remote EDM Indexer”](#) on page 269.

- 4 Proceed with the next step in the EDM process: configuring the Exact Data Profile and indexing the data source.

See [“Creating and modifying Exact Data Profiles”](#) on page 379.

## 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.

See [“Implementing Exact Data Matching”](#) on page 368.

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.

#### 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”](#) on page 374.
- 2 Make sure that you have prepared the data source for indexing.  
See [“Preparing the exact data source file for indexing”](#) on page 376.
- 3 In the Enforce Server administration console, navigate to **Manage > Data Profiles > Exact Data**.
- 4 Click **Add Exact Data Profile**.
- 5 Enter a unique, descriptive **Name** for the profile (limited to 256 characters).  
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.
- 6 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 378.
  - **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 378.
  - **Use This File Name**  
Select this option if you have not yet created the data source file but want to configure EDM rule(s) using a placeholder data source. 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.

---

**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.

See ["Uploading exact data source files to the Enforce Server"](#) on page 378.

- 7 If the first row of your data source contains **Column Names**, select the "Read first row as column names" check box.
- 8 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, five percent), the system quits indexing and displays an indexing error message. If you specify 100% as the error threshold, Symantec Data Loss Prevention indexes the data source without checking for errors.

---

**Note:** Sometimes, a certain percentage of rows in a data set can contain errors. However, more than a small percentage can indicate that the data source file is corrupt, is in an incorrect format, or cannot be read. You can specify that if a certain percentage of rows contains errors, indexing should stop. The default setting is five percent.

---

See ["Preparing the exact data source file for indexing"](#) on page 376.

- 9 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.
- 10 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 runtime when the EDM policy attempts to match inbound data. To make sure that you select the correct encoding, after you click **Next**, verify that the column names appear correctly. If the column names do not look correct, you chose the wrong encoding.

---

- 11 Click **Next** to go to the second **Add Exact Data Profile** screen.
- 12 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 [“Mapping Exact Data Profile fields”](#) on page 384.

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.

- 13 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.

- 14 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.)
- 15** 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.

- 16** 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 [“Scheduling Exact Data Profile indexing”](#) on page 386.

- 17** 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 [“About data owner exception”](#) on page 370.

See [“About field mappings”](#) on page 370.

See [“About index scheduling”](#) on page 371.

See [“About support for character sets, languages, and locales”](#) on page 55.

See [“Configuring the Content Matches Exact Data condition”](#) on page 387.

See [“Creating an EDM profile for remote indexing”](#) on page 271.

## 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 are configuring.

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 18-5** Field mapping options

Field	Description
Data Source Field	<p>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).</p> <p><b>Note:</b> If you are implementing data owner exception, you must map either or both the email address and domain fields.</p> <p>See <a href="#">“Configuring the Content Matches Exact Data condition”</a> on page 387.</p>
System Field	<p>Select the system field for each column.</p> <p>A system field value (except <b>None Selected</b>) cannot be mapped to more than one column.</p> <p>Some system fields have system patterns associated with them (such as social security number) and some do not (such as last name).</p> <p><b>Note:</b> The system does not recognize the pattern XXX-XXX-XXXX 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.</p>

**Table 18-5** Field mapping options (*continued*)

Field	Description
Check mappings against policy template	<p>Select a policy template from the drop-down list to compare the field mappings against and then click <b>Check now</b>.</p> <p>All policy templates that implement EDM appear in the drop-down menu, including any you have imported.</p> <p>See “<a href="#">Choosing an Exact Data Profile</a>” on page 333.</p> <p>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.</p> <p>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.</p>
Advanced View	<p>If you want to customize the schema for the exact data profile, click <b>Advanced View</b> to display the advanced field mapping options.</p> <p><a href="#">Table 18-6</a> lists and describes the additional columns you can specify in the Advanced view screen.</p>
Indexing	<p>Select one of the indexing options.</p> <p>See “<a href="#">Scheduling Exact Data Profile indexing</a>” on page 386.</p>
Finish	<p>Click <b>Finish</b> when you are done configuring the Exact Data Profile.</p>

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 18-6** Advanced View options

Field	Description
Custom Name	<p>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.</p>
Type	<p>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.</p> <p>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.</p>

**Table 18-6** Advanced View options (*continued*)

Field	Description
Description	Click the link ( <b>description</b> ) beside the <b>Type</b> column header to display a pop-up window containing the available system data types.
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 379.

## 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 371.

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 18-7** 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.

**Table 18-7** Scheduling indexing for Exact Data Profiles (*continued*)

Parameter	Description
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	<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. <b>At</b> – Select the hour to start indexing.
Index Daily	<b>At</b> – 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	<b>Day of the week</b> – Select the day(s) to index the document profile. <b>At</b> – 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	<b>Day</b> – Enter the number of the day of each month you want the indexing to occur. The number must be 1 through 28. <b>At</b> – 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.

See “[Mapping Exact Data Profile fields](#)” on page 384.

See “[Creating and modifying Exact Data Profiles](#)” on page 379.

## Configuring the Content Matches Exact Data 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 detection rules. The EDM condition is not available for policy exceptions.

See “[Configuring policies](#)” on page 338.

**Table 18-8**      Configure the Content Matches Exact Data condition

Action	Description
Configure an EDM policy detection rule.	<p>Create a new EDM detection rule in a policy, or modify an existing EDM rule.</p> <p>See <a href="#">“Configuring policy rules”</a> on page 342.</p>
<b>Match Data Rows when All of these match</b>	
Select the fields to match.	<p><b>Check</b> each data field you want the condition to match.</p> <p>Select the number of data fields that must be detected in a message to match this rule.</p> <p>You must select at least as many fields to match as the number of data fields you check.</p> <p>For example, if you select <b>2 of the selected fields</b> from the drop-down menu, you must check at least two fields for detection. You can check more than 2 fields.</p> <p>You can <b>select all</b> or <b>deselect all</b> fields at once.</p>
Select the Where clause to enter specific field values to match (optional).	<p>The <b>Where</b> option matches on the specified field value. Specify the value by selecting an exact data field from the drop-down menu. Enter the value for that field in the adjacent text box. If you enter more than one value, separate the values with commas.</p> <p>For example, consider an exact data profile for "Employees" with a "State" field containing state abbreviations. Select (check) <b>Where</b>, select "State" from the drop-down list, and enter <b>CA,NV</b> in the text box. This rule then causes the detection engine to match a message that contains either <b>CA</b> or <b>NV</b> as content.</p>
<b>Ignore Data Rows when Any of these match</b>	
Ignore data owners.	<p>If you are implementing data owner exception, select one of the options:</p> <ul style="list-style-type: none"> <li>■ <b>Sender matches</b> – Select this option to EXCLUDE the data sender from detection.</li> <li>■ <b>Any or All Recipient matches</b> – Select one of these options to EXCLUDE any or all data recipient(s) from detection.</li> </ul> <p>To except data owners from detection, you must include in your Exact Data Profile either an email address field or a domain address field (for example, symantec.com). Once enabled, if the sender or recipient of confidential information is the data owner (by email address or domain), the detection engine allows the data to be sent or received without generating an incident.</p> <p>See <a href="#">“About data owner exception”</a> on page 370.</p>

**Table 18-8**      Configure the Content Matches Exact Data condition (*continued*)

Action	Description
Exclude data field combinations.	<p>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 <b>_ of the selected fields</b> drop-down menu at the top of the condition configuration.</p> <p>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.</p> <p>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.</p> <p><b>Note:</b> Hold down the Ctrl key to select more than one field in the right-most column.</p>
<b>Additional match condition parameters</b>	
Select an incident minimum.	<p>Enter or modify the minimum number of matches required for the condition to report an incident.</p> <p>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.</p> <p>See <a href="#">“About configuring exact data match counting”</a> on page 371.</p>
Select components to match on.	<p>Select one or more message components to match on:</p> <ul style="list-style-type: none"> <li>■ <b>Envelope</b> – The header of the message.</li> <li>■ <b>Subject</b> – (Not available for EDM.)</li> <li>■ <b>Body</b> – The content of the message.</li> <li>■ <b>Attachments</b> – The content of any files attached to or transported by the message.</li> </ul> <p>See <a href="#">“Selecting components to match on”</a> on page 348.</p>
Select one or more conditions to also match.	<p>Select this option to create a compound condition. All conditions must match for the rule to trigger an incident.</p> <p>You can <b>Add</b> any available condition from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

See [“EDM best practices”](#) on page 390.

## EDM best practices

Exact Data Matching (EDM) is one of the most powerful types of detection. You can use EDM to exactly match data from a database, spreadsheet, or keyword list. Examples of such data might include social security numbers, last names, account numbers, and so on. These data profiles might contain millions of rows of information.

Although there is no limit to the number of columns you can in your EDM index, it is recommended that you have a 2-3 column index containing the key identifiers you want to match. For example, first name is generally not a good column to include in an index because there is likely to be too much duplication among records. Properly indexed identifiers yield the high degrees of accuracy.

An EDM rule performs a full-text search against the message, checking each word (except those that are excluded) for potential matches. The matching algorithm compares each individual word in the message with the contents of each cell in the data profile. If a cell in the data profile contains multiple words, that cell can never match a word in a message. This behavior is because the matching algorithm cannot match individual words to a group of words.

The exception is that certain types of text trigger a tabular search. For example, when the message is decomposed, it might have certain comma- or pipe-separated data or an Excel file attachment. In that case, each cell (or piece of data) is individually tested against the data profile, even if the cell contains multiple words. For example, an address can match.

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.

Think about the column combinations that result from the selections. For example, two or more of social security number, first name, phone number, or last name contain lots of potentially worthless combinations. (This may include first name + phone number, phone number + last name, and first name + last name). To ensure that you generate useful incidents, tune the policy by requiring more columns (that is, require three or more items to be present). Alternatively you can use exceptions to exclude the combinations that do not present a concern.

The column exceptions are available only when you select two or three columns or more. 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.

A match always comes from the same row. For example, if the rule specifies two or more of last name and social security number, the engine detects only those social security numbers that correspond to last names.

Generally, databases are organized into tables with columns and rows. Each column contains a particular type of data. Each row represents one record, which contains related values for each column data type. Some columns of data can contain more than one word. For example, the column City might contain the words San Francisco. Currently, Symantec Data Loss Prevention detects multiple-word data only if it appears in tabular formatted data, such as in an Excel file. This limitation applies to database rules only, not to pattern rules.

See [“About implementing Exact Data Matching”](#) on page 368.



# Detecting content using Index Document Matching

This chapter includes the following topics:

- [About implementing Indexed Document Matching](#)
- [Detectable content types](#)
- [Manage and add Indexed Document Profiles](#)
- [Implementing Indexed Document Matching](#)
- [Preparing the document source for indexing](#)
- [Excluding \(whitelisting\) content from detection](#)
- [Creating and modifying Indexed Document Profiles](#)
- [Filtering documents by file name and size](#)
- [Scheduling document profile indexing](#)
- [Configuring the Content Matches Document Signature condition](#)
- [IDM best practices](#)

## About implementing Indexed Document Matching

To implement Indexed Document Matching, you first identify the documents that contain the specific content you want to protect. You then index these documents using the Enforce Server administration console. The indexing process extracts the content, normalizes it, and fingerprints it. You then configure the "Content Matches Document Signature From" detection rule to detect the extracted portions of an original protected document, drafts, or different versions of protected

document content. Indexed Document Matching provides the ability to exclude ("whitelist") content such as standard boilerplate text to fine-tune detection results and reduce false positives.

See [“Implementing Indexed Document Matching”](#) on page 402.

Use Indexed Document Matching (IDM) to fingerprint and detect specific data from sensitive documents. For example, you can use IDM to protect the documents that contain proprietary software code, research specifications, or merger and acquisition documents. You can author a policy to detect a match when a message contains the entire document or a section of a document. To use IDM, you create a secure Document Index that contains hashed data from your source. This index is then referenced in detection rules in one or more policies. Your policies then use the index in production at runtime.

See [“Manage and add Indexed Document Profiles”](#) on page 400.

To detect specific documents, Symantec Data Loss Prevention requires a special indexed version of the documents. An Indexed Document Profile is a secure file (or set of files) containing hashes of text passages from one or more source documents. Collectively, the hashes for a single document are called the document fingerprint. The index does not contain actual document content, so it is secure. Symantec Data Loss Prevention compares the index to documents on your network. The detection engine can detect an exact match or a partial match. Exact matching is used for binary files, such as .gif, .mpg, .avi.

Indexes consist of one or more secure, binary .rdx files, each large enough to fit into random access memory (RAM) on the detection server(s). For a large document, Symantec Data Loss Prevention may break up the data into several .rdx files. In production, Symantec Data Loss Prevention converts input content into hashed text passages using the same algorithm it employs for indexes. It then compares passages from input content to those in the appropriate .rdx files, identifying matches. A partial match means that Symantec Data Loss Prevention detects part of the indexed text in an input document. Symantec Data Loss Prevention can perform partial matching only on text documents (as opposed to audio or to video files, for example).

Symantec Data Loss Prevention stores document indexes in

`C:\Vontu\Protect\index` (on Windows) or in `/var/Vontu/index` (on Linux) on the Enforce Server. And it stores indexes on all detection servers. Symantec Data Loss Prevention deploys indexes only when you include them in a policy and then enable the policy on a detection server. When the policy is active, the detection server loads the index into RAM.

As soon as you create a document profile, you can reference it in a policy. However, you must index the document before Symantec Data Loss Prevention can detect it in production.

See “[Detectable content types](#)” on page 395.

## Detectable content types

The following tables list the types of file formats whose content Symantec Data Loss Prevention can detect.

**Table 19-1** Word processing file formats that can be analyzed

Format Name	Format Extension
Adobe FrameMaker Interchange Format	MIF
Apple iWork Pages	PAGES
Applix Words	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 Professional Write Plus	AMI
Lotus Word Pro	LWP
Lotus SmartMaster	MWP
Microsoft Word PC	DOC
Microsoft Word Windows	DOC
Microsoft Word Windows XML	DOCX

**Table 19-1** Word processing file formats that can be analyzed (*continued*)

<b>Format Name</b>	<b>Format Extension</b>
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
OpenOffice Writer	SXW
OpenOffice Writer	ODT
StarOffice Writer	SXW
StarOffice Writer	ODT
WordPad	RTF
XML Paper Specification	XPS
XyWrite	XY4

**Table 19-2** Presentation file formats that can be analyzed

<b>Format Name</b>	<b>Format Extension</b>
Apple iWork Keynote	KEYNOTE
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

**Table 19-2** Presentation file formats that can be analyzed (*continued*)

<b>Format Name</b>	<b>Format Extension</b>
Microsoft PowerPoint Windows Macro-Enabled XML Template	POTM
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

**Table 19-3** Spreadsheet file formats that can be analyzed

<b>Format Name</b>	<b>Format Extension</b>
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

**Table 19-3** Spreadsheet file formats that can be analyzed *(continued)*

Format Name	Format Extension
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

**Table 19-4** Encapsulation file formats that can be analyzed

Format Name	Format Extension
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

**Table 19-5** Text and markup file formats that can be analyzed

Format Name	Format Extension
ANSI	TXT
ASCII	TXT
HTML	HTM
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	HTM
XML (generic)	XML

**Table 19-6** Email file formats that can be analyzed

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

**Table 19-7** Computer-aided design (CAD) file formats that can be analyzed

Format Name	Format Extension
AutoCAD Drawing	DWG

**Table 19-7** Computer-aided design (CAD) file formats that can be analyzed  
*(continued)*

Format Name	Format Extension
AutoCAD Drawing Exchange	DFX
Microsoft Visio	VSD
Microstation	DGN

**Table 19-8** Graphics file formats that can be analyzed

Format Name	Format Extension
Enhanced Metafile	EMF
Lotus Pic	PIC
Tagged Image File (metadata only)	TIFF
Windows Metafile	WMF

**Table 19-9** Database file formats that can be analyzed

Format Name	Format Extension
Microsoft Access	MDB
Microsoft Project (metadata only)	MPP

**Table 19-10** Other file formats that can be analyzed

Format Name	Format Extension
Adobe PDF	PDF
MPEG-1 Audio layer 3 (metadata only)	MP3
Microsoft Windows Backup Utility File	BKF

## 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.

See [“About implementing Indexed Document Matching”](#) on page 393.

**Table 19-11** Indexed Documents screen actions

Column	Description
Add IDM profile	Click <b>Add Document Profile</b> to create a new Indexed Document Profile. See <a href="#">“Implementing Indexed Document Matching”</a> on page 402.
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 <a href="#">“Creating and modifying Indexed Document Profiles”</a> on page 405.
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 19-12** Indexed Documents screen details

Column	Description
Document Profile	The name of the document data profile.
Detection server	The name of the detection server that indexes the Document Profile and the Document Profile version.  Click the <b>triangle icon</b> 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 19-12** Indexed Documents screen details (*continued*)

Column	Description
Status	<p>The current status of the document indexing process, which can be any of the following:</p> <ul style="list-style-type: none"> <li>■ Next scheduled indexing (if it is not currently indexing)</li> <li>■ Sending an index to a detection server</li> <li>■ Indexing</li> <li>■ Deploying to a detection server</li> </ul> <hr/> <p>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:</p> <ul style="list-style-type: none"> <li>■ Completed, including a completion date</li> <li>■ Pending index completion (that is, waiting for the Enforce Server to finish indexing a file)</li> <li>■ Replicating indexing</li> <li>■ Creating index (internally)</li> <li>■ Building caches</li> </ul>
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 [“About Data Profiles”](#) on page 316.

See [“Scheduling document profile indexing”](#) on page 409.

See [“Configuring the Content Matches Document Signature condition”](#) on page 411.

## Implementing Indexed Document Matching

To implement IDM

- 1 Prepare the documents for indexing.  
 See [“Preparing the document source for indexing”](#) on page 403.
- 2 Optionally, configure Symantec Data Loss Prevention to whitelist specified text during indexing and detection.  
 See [“Excluding \(whitelisting\) content from detection”](#) on page 404.
- 3 Create a document profile (in the Enforce Server Admin Console) that specifies the document source.  
 See [“Creating and modifying Indexed Document Profiles”](#) on page 405.

- 4 Configure any document source filters.  
 See [“Filtering documents by file name and size”](#) on page 408.
- 5 Schedule indexing as necessary.  
 See [“Scheduling document profile indexing”](#) on page 409.
- 6 Configure an IDM rule and policy.  
 See [“Configuring the Content Matches Document Signature condition”](#) on page 411.

## Preparing the document source for indexing

A document source is a ZIP archive file that contains documents to index. It can also be the files in a file share on a local or on a remote computer. A document source archive 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. You can also specify file name and file-size filters in the document profile. The filters tell the system which files to include or ignore during indexing.

### To prepare the document source for indexing

- 1 Create the document source archive file that contains the documents you want to protect. Do not include any internal archive file within the document source archive file. Any internal archive file is not opened and indexed.
- 2 To protect a large collection of documents, separate these documents across share directories or file archives. Then, create a separate document profile for each directory or archive.

A large document source can affect performance during the indexing process. To reduce the load during indexing, Symantec Data Loss Prevention limits the size of each document source to approximately 300,000 or 400,000 documents. The exact number of documents Symantec Data Loss Prevention permits depends on the average extracted text size (per document source).

- 3 To have the document source appear in a convenient drop-down list on the **Add Document Profile** screen, copy it to one of the following directories:
  - On Windows, copy it to `Vontu_home\Protect\documentprofiles` (for example, `C:\Vontu\Protect\documentprofiles`).

- On Linux, copy it to `/var/Vontu/documentprofiles`.
- 4 Proceed with the next step of the process: configuring the document profile. Alternatively, if you want to exclude specific document content from detection, whitelist it.  
  
See “[Creating and modifying Indexed Document Profiles](#)” on page 405.  
See “[Excluding \(whitelisting\) content from detection](#)” on page 404.

## Excluding (whitelisting) content from detection

Often sensitive documents contain standard boilerplate text that that does not requires protection. In this case you can configure the system to exclude ("whitelist") this text. The Enforce Server does not index whitelisted text and thus excludes it from detection. If you want to exclude certain text from detection in a particular document source, you must perform the steps in this section before indexing.

To exclude document content from detection, create a `Whitelisted.txt` file for each Document Profile you want to index. When you index the document source, the Enforce Server looks for the `Whitelisted.txt` file. If such a file exists, the Enforce Server copies it to `Whitelisted.x.txt`, where `x` is a unique Document Profile identification number. Future indexing of the same profile uses the profile-specific whitelist file, not a common file.

### To whitelist document content

- 1 Copy all the content you want to whitelist into a text file and save the file as `Whitelisted.txt`.
- 2 Save the file to the appropriate directory:
  - On Windows, save it to `Vontu_home\Protect\documentprofiles\whitelisted`. *Vontu\_home* is the Symantec Data Loss Prevention installation directory. For example, save the file to `c:\Vontu\Protect\documentprofiles\whitelisted`.
  - On Linux, save the file to `/var/Vontu/documentprofiles/whitelisted`.

By default, a file you index 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.

---

**Note:** 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.

---

### To change the default minimum for whitelisted text

- 1 On the Symantec Data Loss Prevention host, navigate to `Vontu_home\Protect\config`. For example, on Windows go to `c:\Vontu\Protect\config`. Or, on Linux go to `/opt/Vontu/Protect/config`.
- 2 Use a text editor to open the `Indexer.properties` file, and locate the following text:

```
# Guarantee threshold t
com.vontu.profiles.documents.t=130
```

- 3 Change the numerical portion of the `Guarantee threshold t` 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
```

- 4 Save the file.

See [“Creating and modifying Indexed Document Profiles”](#) on page 405.

## Creating and modifying Indexed Document Profiles

You define and configure a Document Profile at the **Manage > Data Profiles > Indexed Documents > Configure Document Profile** screen.

The Document Profile specifies the source document(s), the indexing parameters, and the indexing schedule. You must define an appropriate Document Profile to implement Content Matches Document Signature detection.

### To configure a document profile

- 1 Log on to the Enforce Server Administration Console with policy authoring privileges.
- 2 Navigate to the **Manage > Data Profiles > Indexed Documents** screen.

- 3 At the **Indexed Documents** screen, click **Add Document Profile**.  
Or, click an existing Document Profile to edit it.  
See “[Manage and add Indexed Document Profiles](#)” on page 400.
- 4 Enter a **Name** for the Document Profile. For easy reference, choose a name that describes the data content and the index type (for example, Research Docs IDM). The name of the document profile is limited to 256 characters.
- 5 Each document profile is a group of files that you want to protect. Before you can use a document profile in a policy, copy the document profile files to Enforce and add a document profile that references it.

Specify the data source by selecting one of the following options:

■ **Upload Document Archive to Server Now**

Type the full path and file name of the document archive (.zip file) or click **Browse** to select it. For example, enter `c:\Documents\Research.zip`. If you edit a Document Profile and change the data source file, an **Upload Now** option appears. After you specify the new file location, click **Upload Now**.

---

**Note:** If a file inside the archive is another archive file (\*.zip), Symantec Data Loss Prevention does not unzip and index it. The embedded archive is considered for exact matches only, like image files and other unsupported file formats.

---

---

**Note:** The maximum size of the archive file is limited only by the disk space that you allocate to the Enforce Server. The maximum upload is 2 GB; however, any file over 50 MB is not recommended. Large files can take a long time to upload. If your archive file is over 50 MB, copy it to the Enforce Server using a third-party solution (such as Secure FTP). You can then select this file from the **Use Local Path on Manager** pull-down menu.

---

■ **Reference Archive on Enforce Server**

If you copied the document source to the Symantec Data Loss Prevention document files directory, you can select the document source from the drop-down list. Any document sources currently referenced by another document profile do not appear on the drop-down list.

See “[Preparing the document source for indexing](#)” on page 403.

■ **Use Local Path on Enforce Server**

Type the path to the directory that contains the documents to index. For example, type `c:\Documents`. You must specify the exact path, not a

relative path. Do not include the actual file names in the path. Note that you cannot use this method to index the documents that are contained in a .zip file.

■ **Use Remote SMB Share**

Enter the Universal Naming Convention (UNC) path for the Server Message Block (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.) Enter a valid user name and password for the share, and then re-enter the password.

---

**Note:** 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 in the pull-down menu.

See [“About the credential store”](#) on page 99.

- 6 In the **File Name Include Filters** and the **File Name Exclude Filters** text boxes, enter any filters you want to use. For example, enter \*.doc in the **File Name Include Filters** text box to have Symantec Data Loss Prevention index only \*.doc files in the document source.

See [“Filtering documents by file name and size”](#) on page 408.

- 7 In the **Size Filters** fields, specify any restrictions on the size of files Symantec Data Loss Prevention should index. For example, to prevent indexing of files larger than 2 megabytes, enter 2 in the **Ignore Files Larger Than** field and select MB from the corresponding drop-down list. To prevent Symantec Data Loss Prevention from indexing files smaller than one kilobyte, enter 1 in the **Ignore Files Smaller Than** field and select KB from the drop-down list.

- 8 In the **Indexing** section, select one of the following options:

■ **Submit Indexing Job on Save**

Causes Symantec Data Loss Prevention to index the document when you save the Document Profile.

■ **Submit Indexing Job on Schedule**

Causes Symantec Data Loss Prevention to display schedule options. Make a selection from the Schedule drop-down list and specify days, dates, and times as required.

See “[Scheduling document profile indexing](#)” on page 409.

**9 Click Finish.**

After Symantec Data Loss Prevention finishes indexing, it deletes the document source from the Enforce Server. For example, Symantec Data Loss Prevention deletes a document source archive file from

`c:\Vontu\Protect\documentprofiles` (on Windows) or  
`/var/Vontu/documentprofiles` (on Linux).

---

**Note:** Symantec Data Loss Prevention does not delete documents if you chose **Use Remote SMB Share**.

---

## Filtering documents by file name and 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 Size Filters.

**File Name Filters:**

- If the File Name Include Filters field is empty, matching is performed on all documents in the specified document profile. If you enter anything in the field, it is treated as an inclusion filter. In this case the document is indexed only if it matches the filter you specify.
- The detection server ignores all text that you specify in the File Name Exclude Filters field.
- When you use file name filters, Symantec recommends to select either exclusion filters or inclusion filters, not both.

[Table 19-13](#) describes the syntax accepted by the **File Name Filters** feature.

**Table 19-13** 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.

For **File Name Filters**, Symantec Data Loss Prevention treats forward slashes (/) and backslashes (\) as equivalent. It 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.

The following list includes sample filters and descriptions of behavior if you enter them in the **File Name Include Filters** field:

**Table 19-14** File name filter examples

Filter	Description
*.txt,*.doc	The system indexes only .txt and .doc files in the .zip file or file share, ignoring everything else.
?????.doc	The system indexes files with the .doc extension and files with five-character names, such as hello.doc and stats.doc (but not good.doc or foobar.doc).
*/documentation/*,*/specs/*	The system indexes only files in two subdirectories below the root directory, one called "documentation" and the other called "specs."

Use the size filters to exclude files from the matching process based on their size. Any files that match the size filters are ignored.

[Table 19-15](#) describes the file size filter options.

**Table 19-15** File size filter configuration options

Filter	Description
Ignore Files Smaller Than	To exclude files smaller than a particular size, enter a number in this field.  Select the appropriate unit of measure Bytes, KB (kilobytes), or MB (megabytes) from the drop-down list next to it.
Ignore Files Larger Than	To exclude files larger than a particular size, enter a number in this field.  Select the appropriate unit of measure (Bytes, KB, or MB) from the drop-down list next to it.

## Scheduling document profile indexing

As part of creating a document profile, you can set up a schedule for indexing the document source.

When you configure a document profile, select **Submit Indexing Job on Save** to index the document profile as soon as you save it (recommended). Alternatively, you can set up a schedule for indexing the document source.

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.

---

**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.

---

To schedule document indexing, select **Submit Indexing Job on Schedule** and select a schedule from the drop-down list as described in [Table 19-16](#).

**Table 19-16** Options for scheduling Document Profile indexing

Parameter	Description
Index Once	<p><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.</p> <p><b>At</b> – Select the hour to start indexing.</p>

**Table 19-16** Options for scheduling Document Profile indexing (*continued*)

Parameter	Description
Index Daily	<p><b>At</b> – Select the hour to start indexing.</p> <p><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.</p>
Index Weekly	<p><b>Day of the week</b> – Select the day(s) to index the document.</p> <p><b>At</b> – Select the hour to start indexing.</p> <p><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.</p>
Index Monthly	<p><b>Day</b> – Enter the number of the day of each month you want the indexing to occur. The number must be 1 through 28.</p> <p><b>At</b> – Select the hour to start indexing.</p> <p><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.</p>

## Configuring the Content Matches Document Signature condition

The Content Matches Document Signature matches unstructured document content based on specified document source called the Document Profile.

See [“About implementing Indexed Document Matching”](#) on page 393.

The Content Matches Document Signature is available for detection rules and exceptions.

See [“Configuring policies”](#) on page 338.

### 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 policy rules”](#) on page 342.
  - See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the IDM condition parameters.
  - See [Table 19-17](#) on page 412.
- 3 Save the policy configuration.

**Table 19-17** Content Matches Document Signature condition parameters

Action	Description
Set the Minimum Document Exposure.	Select an option from the drop-down list.  Any number you select indicates the percentage of the match. If you select <b>Exact</b> , only the documents whose content matches the content of a source document exactly are considered a match.
Configure Match Counting.	Select how you want to count matches: <ul style="list-style-type: none"> <li>■ <b>Check for existence</b> Reports a match count of 1 if there are one or more condition matches.</li> <li>■ <b>Count all matches</b> Reports a match count of the exact number of matches.</li> </ul> See “ <a href="#">Configuring match counting</a> ” on page 346.
Select the components to Match On.	Select one of the available message components to match on: <ul style="list-style-type: none"> <li>■ <b>Body</b> – The content of the message.</li> <li>■ <b>Attachments</b> – Any files attached to or transferred by the message.</li> </ul> See “ <a href="#">Selecting components to match on</a> ” on page 348.
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.

See “[IDM best practices](#)” on page 412.

## IDM best practices

If Symantec Data Loss Prevention is unable to index the content of a document (for example, an image file), the detection performs exact matching. This behavior is true even if you select a minimum document exposure percentage that is less than exact. In addition, the detection engine uses exact matching for very small files, even if these files are text files. (The exact length is variable depending on the content of the file. Generally, it is around 300 characters or less.)

For example, consider a document source that contains five Microsoft Word documents, one Microsoft Excel document, and three image files. You select 50 percent for the Minimum Document Similarity. Symantec Data Loss Prevention indexes the Word and Excel documents and looks for 50 percent matches for those documents. In contrast it looks for exact data matches for the three image files.

For the 50 percent exposure, if a document contains roughly 50 percent of the content in the selected document profile, it is considered a match.

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.

---

**Note:** 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 someone pastes its contents into the body of an email message or creates a PDF from the Word document, the engine considers it a match.

---

See [“About implementing Indexed Document Matching”](#) on page 393.



# Detecting content using data identifiers

This chapter includes the following topics:

- [About data identifiers](#)
- [Available system data identifiers](#)
- [About data identifier breadths](#)
- [About optional validators](#)
- [Acceptable characters for optional validators](#)
- [About cross-component matching for data identifiers](#)
- [About modifying data identifiers](#)
- [About data identifier patterns](#)
- [About validators](#)
- [About custom data identifiers](#)
- [About data normalizers](#)
- [About data identifier configuration](#)
- [Manage and add data identifiers](#)
- [Configuring the Content Matches Data Identifier condition](#)
- [Selecting system data identifier breadth](#)
- [Configuring optional validators](#)

- [Modifying and creating data identifiers](#)
- [Manually cloning a system data identifier before modifying it](#)
- [Editing required validator input](#)
- [Implementing custom data identifiers](#)
- [Implementing patterns to match data](#)
- [Selecting required data validators](#)
- [Implementing custom script validators](#)
- [Data identifier best practices](#)

## About 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.

See [“Selecting system data identifier breadth”](#) on page 436.

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.

**Table 20-1** Categories of data identifiers

Category	Description
Personal Identity	Detect various types of identification numbers for the regions of North America, Europe, and Asia Pacific. See <a href="#">Table 20-2</a> on page 417. See <a href="#">Table 20-6</a> on page 419. See <a href="#">Table 20-7</a> on page 420.
Financial	Detect financial identification numbers, such as credit card numbers and ABA routing numbers. See <a href="#">Table 20-3</a> on page 418.
Healthcare	Detect U.S. and international drug codes. See <a href="#">Table 20-4</a> on page 419.
Information Technology	Detect IP addresses. See <a href="#">Table 20-5</a> on page 419.
International Keywords	Detect and validate common international content using keywords. See <a href="#">“Using find keywords for international system data identifiers”</a> on page 531.
Modified	System-defined data identifiers that you modify. See <a href="#">“About modifying data identifiers”</a> on page 425.
Custom	User-defined data identifiers. See <a href="#">“Implementing custom data identifiers”</a> on page 443.

## Available system data identifiers

Symantec Data Loss Prevention provides 36 system-defined data identifiers to help you accurately detect and validate pattern-based sensitive data.

**Table 20-2** North American personal identity

Data identifier	Description
US Social Security Number (SSN)	See <a href="#">“US Social Security Number (SSN) system data identifier”</a> on page 596.
Canadian Social Insurance Number	See <a href="#">“Canadian Social Insurance Number system data identifier”</a> on page 541.

**Table 20-2** North American personal identity (*continued*)

Data identifier	Description
US Individual Tax ID Number (ITIN)	See “ <a href="#">UK Tax ID Number system data identifier</a> ” on page 591.
Driver's License Number – CA State	See “ <a href="#">Drivers License Number – CA State system data identifier</a> ” on page 554.
Driver's License Number – IL State	See “ <a href="#">Drivers License Number - IL State system data identifier</a> ” on page 557.
Driver's License Number – NJ State	See “ <a href="#">Drivers License Number - NJ State system data identifier</a> ” on page 559.
Driver's License Number – NY State	See “ <a href="#">Drivers License Number - NY State system data identifier</a> ” on page 560.
Driver's License Number – FL, MI, MN States	See “ <a href="#">Drivers License Number - FL, MI, MN States system data identifier</a> ” on page 556.

**Table 20-3** Financial

Data identifier	Description
Credit Card Number	See “ <a href="#">Credit Card Number system data identifier</a> ” on page 546.
ABA Routing Number	See “ <a href="#">ABA Routing Number system data identifier</a> ” on page 536.
CUSIP Number	See “ <a href="#">CUSIP Number system data identifier</a> ” on page 552.
SWIFT Code	See “ <a href="#">SWIFT Code system data identifier</a> ” on page 578.
Credit Card Magnetic Stripe Data	See “ <a href="#">Credit Card Magnetic Stripe Data system data identifier</a> ” on page 544.
IBAN West	See “ <a href="#">IBAN West system data identifier</a> ” on page 568.
IBAN Central	See “ <a href="#">IBAN Central system data identifier</a> ” on page 563.
IBAN East	See “ <a href="#">IBAN East system data identifier</a> ” on page 565.

**Table 20-4** Healthcare

Data identifier	Description
National Drug Code	See <a href="#">“National Drug Code (NDC) system data identifier”</a> on page 572.
Australian Medicare Number	See <a href="#">“Australian Medicare Number system data identifier”</a> on page 539.

**Table 20-5** Information technology

Data identifier	Description
IP Address	See <a href="#">“IP Address system data identifier”</a> on page 570.

**Table 20-6** European personal identity

Data identifier	Description
Codice Fiscale	See <a href="#">“Codice Fiscale system data identifier”</a> on page 543.
Spanish DNI ID	See <a href="#">“Spanish DNI ID system data identifier”</a> on page 577.
Burgerservicenummer	See <a href="#">“Burgerservicenummer system data identifier”</a> on page 540.
UK Driver's License Number	See <a href="#">“UK Drivers License Number system data identifier”</a> on page 581.
UK Tax ID Number	See <a href="#">“UK Tax ID Number system data identifier”</a> on page 591.
UK Passport Number	See <a href="#">“UK Passport Number system data identifier”</a> on page 589.
UK National Insurance Number	See <a href="#">“UK National Insurance Number system data identifier”</a> on page 586.
UK National Health Service (NHS) Number	See <a href="#">“UK National Health Service (NHS) Number system data identifier”</a> on page 584.
UK Electoral Roll Number	See <a href="#">“UK Electoral Roll Number system data identifier”</a> on page 583.
French INSEE Code	See <a href="#">“French INSEE Code system data identifier”</a> on page 562.

**Table 20-6** European personal identity (*continued*)

Data identifier	Description
Swiss AHV Number	See <a href="#">“Swiss AHV Number system data identifier”</a> on page 580.

**Table 20-7** Asia Pacific personal identity

Data identifier	Description
Australian Tax File Number	See <a href="#">“Australian Tax File Number system data identifier”</a> on page 540.
People's Republic of China ID	See <a href="#">“People's Republic of China ID system data identifier”</a> on page 575.
Hong Kong ID	See <a href="#">“Hong Kong ID system data identifier”</a> on page 562.
Singapore NRIC	See <a href="#">“Singapore NRIC system data identifier”</a> on page 575.
South Korean Resident Registration Number	See <a href="#">“South Korea Resident Registration Number system data identifier”</a> on page 576.
Taiwan ROC ID	See <a href="#">“Taiwan ROC ID system data identifier”</a> on page 580.

## 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 [Table 20-8](#) on page 421.

For example, the US Social Security Number (SSN) data identifier provides three breadths of detection: wide, medium, and narrow. The Driver's License Number – CA State system Data Identifier provides wide and medium breadths. In both cases the narrowest breadth implements 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 system data identifier breadth”](#) on page 436.

**Table 20-8** Available rule breadths for system data identifiers

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.

## About optional validators

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 [Table 20-9](#) on page 421.

The type of characters accepted by each optional validator depends on the data identifier.

See [“Acceptable characters for optional validators”](#) on page 422.

**Note:** Optional validators only apply to the policy instance you are actively configuring; they do not apply system-wide.

**Table 20-9** Available optional validators for policy instances

Optional validator	Description
Require beginning characters	Match the characters that begin (lead) the matched data item. 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 <a href="#">“Acceptable characters for optional validators”</a> on page 422.

**Table 20-9** Available optional validators for policy instances (*continued*)

Optional validator	Description
Require ending characters	Match the characters that end (trail) the matched data item. See <a href="#">“Acceptable characters for optional validators”</a> on page 422.
Exclude beginning characters	Exclude from matching characters that being (lead) the matched data. See <a href="#">“Acceptable characters for optional validators”</a> on page 422.
Exclude ending characters	Exclude from matching the characters that end (trail) the matched data item. See <a href="#">“Acceptable characters for optional validators”</a> on page 422.
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 report a match.  See <a href="#">“About cross-component matching for data identifiers”</a> on page 425.  This optional validator accepts any characters (numbers, letters, others).  See <a href="#">“Acceptable characters for optional validators”</a> on page 422.

## Acceptable characters for optional validators

Each optional validator requires you to enter in some data values. You must enter the appropriate type of data.

See [“About optional validators”](#) on page 421.

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 440.

---

**Note:** The **Find keyword** optional validator accepts any characters as values for all data identifiers.

---

**Table 20-10** Acceptable characters for optional validators

<b>Data Identifier</b>	<b>Require ending characters</b>	<b>Exclude ending characters</b>	<b>Require beginning characters</b>	<b>Exclude beginning characters</b>
US Social Security Number (SSN)	Numbers only			
Canadian Social Insurance Number	Numbers only			
US Individual Tax Identification Number (ITIN)	Numbers only			
Driver's License Number – CA State	Numbers only		Any characters (normalized to lowercase)	
Driver's License Number – IL State	Numbers only		Any characters (normalized to lowercase)	
Driver's License Number – NJ State	Numbers only		Any characters (normalized to lowercase)	
Driver's License Number – NY State	Numbers only			
Driver's License Number – FL, MI, MN States	Numbers only		Any characters (normalized to lowercase)	
Credit Card Number	Numbers only			
ABA Routing Number	Numbers 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			

**Table 20-10** Acceptable characters for optional validators (*continued*)

<b>Data Identifier</b>	<b>Require ending characters</b>	<b>Exclude ending characters</b>	<b>Require beginning characters</b>	<b>Exclude beginning characters</b>
Australian Medicare Number			Numbers 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	
UK National Insurance Number			Alphanumeric (normalized to lowercase)	
UK National Health Service (NHS) Number			Numbers only	
UK Electoral Roll Number		Numbers only	Any characters (normalized 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 ROC ID			Numbers only	

## About cross-component matching for data identifiers

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 [“About message components that can be matched”](#) on page 293.

For example, consider a scenario where you implement the narrow breadth edition of the 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 434.

## About modifying data identifiers

You can modify data identifiers to suit your requirements. You can modify the system-defined data identifiers, 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.

See [“Modifying and creating data identifiers”](#) on page 441.

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.

See [“Editing required validator input”](#) on page 442.

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.

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, you should consider manually cloning it.

See [“Manually cloning a system data identifier before modifying it”](#) on page 442.

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.

## About data identifier patterns

Data identifiers implement patterns to match content. The pattern syntax is similar to regular expressions, but more limited. For example, the data identifier pattern syntax does not support some regular expression features, including grouping, lookahead and lookbehind, and many special characters (notably ".").

You can edit the patterns for system data identifiers, and you can write your own custom patterns.

See [“Implementing patterns to match data”](#) on page 444.

The system-defined data identifier patterns have been tuned and optimized for precise content matching. The best way to understand how to write patterns is to examine the system-defined data identifier patterns.

See [“Selecting system data identifier breadth”](#) on page 436.

---

**Note:** The system only allows the use of ASCII characters for data identifier patterns.

---

## About validators

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 [Table 20-11](#) on page 427.

When you modify a data identifier, you can edit the input values for any validator that accepts data. Validators marked with an asterisk (\*) beside the name in the table below require data input.

See [“Editing required validator input”](#) on page 442.

When you modify a data identifier, you can add and remove data 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 required data validators”](#) on page 445.

**Table 20-11** Available validators for system and custom data identifiers

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 <a href="#">“Implementing custom script validators”</a> on page 446.
DNI control key check	Computes the control key and checks if it is valid.
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.

**Table 20-11** Available validators for system and custom data identifiers  
*(continued)*

Validator	Description
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.
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.
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.
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.

**Table 20-11** Available validators for system and custom data identifiers  
(continued)

Validator	Description
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 9th position must be larger than 00 and smaller than 32.
UK NHS	UK NHS checksum.

## About custom data identifiers

You can define your own data identifiers. To create a custom data identifier, you implement one or more detection pattern(s), select one or more data validators (optional), provide the data input if the validator requires it, and choose a data normalizer.

Once configured, policy authors can use custom data identifiers in one or more policies.

See [“Implementing custom data identifiers”](#) on page 443.

**Table 20-12** Custom data identifier components

Component	Description
Patterns	Define one or more regular expression patterns, separated by line breaks.
Validators	Add or remove validators to perform validation checks on the data detected by the pattern(s).

**Table 20-12** Custom data identifier components (*continued*)

Component	Description
Data Entry	Provide comma separated data values for any validators that require data input.
Normalizer	Select a normalizer to standardize the data before matching against it.

## About data normalizers

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. [Table 20-13](#) lists and describes the normalizers you can implement for custom data identifiers.

---

**Note:** You cannot modify the normalizer of a system-defined data identifier.

---

**Table 20-13** Available data normalizers

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.

## About data identifier configuration

You can configure three types of data identifiers:

- Instance – defined at the policy level
- Modified – configured at the system-level
- Custom – created at the system-level

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.

---

**Note:** The system does export modified and custom data identifiers in a policy template. The system exports a reference to a system data identifier. The target system where the policy template is imported provides the actual data identifier.

---

Data identifier configuration done at the policy instance-level is specific to that policy.

See [“Configuring the Content Matches Data Identifier condition”](#) on page 434.

**Table 20-14** Policy instance configuration options

Selectable at the policy level	Not configurable
<ul style="list-style-type: none"> <li>■ <b>Breadth</b> You can implement any breadth the data identifier supports at the instance level.</li> <li>■ <b>Optional Validators</b> You can select one or more optional validators at the instance level.</li> </ul>	<ul style="list-style-type: none"> <li>■ <b>Patterns</b> You cannot modify the match patterns at the instance level.</li> <li>■ <b>Active Validators</b> You cannot modify, add, or remove required validators at the instance level.</li> </ul>

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.

See [“Modifying and creating data identifiers”](#) on page 441.

**Table 20-15** System data identifier modification options

Modifiable at the system level	Not configurable
<ul style="list-style-type: none"> <li>■ <b>Patterns</b> You can edit one or more data identifier patterns at the system level.</li> <li>■ <b>Active Validators</b> You can add or remove required validators at the system level.</li> <li>■ <b>Data Entry</b> You can edit the input of an active validator for a system data identifier.</li> </ul>	<ul style="list-style-type: none"> <li>■ <b>Name, Description, and Category</b> You cannot modify the name, description, or category of a system data identifier.</li> <li>■ <b>Breadth</b> You cannot define a new detection breadth for a system data identifier; you can only modify an existing breadth.</li> <li>■ <b>Optional Validators</b> You cannot define optional validators at the system level. You can only configure optional validators at the policy level.</li> <li>■ <b>Data Normalizer</b> You cannot modify the type of data normalizer implemented by a system data identifier.</li> <li>■ <b>Delete</b> You cannot delete a system data identifier.</li> </ul>

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 [“Implementing custom data identifiers”](#) on page 443.

**Table 20-16** Custom data identifier implementation options

Configurable at the custom level	Not configurable
<ul style="list-style-type: none"> <li>■ <b>Name and Description</b>                      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.</li> <li>■ <b>Patterns</b>                      You must define at least one pattern for the custom data identifier to be valid.</li> <li>■ <b>Active Validators</b>                      You can add one or more required validators to a custom data identifier.</li> <li>■ <b>Data Entry</b>                      You can edit the input of an active validator that accepts data input.</li> <li>■ <b>Data Normalizer</b>                      You must select a data normalizer when defining a custom data identifier.</li> </ul>	<ul style="list-style-type: none"> <li>■ <b>Category</b>                      The system assigns a custom data identifier to the <b>Custom</b> category. You cannot change this setting.</li> <li>■ <b>Breadth</b>                      The system assigns a custom data identifier to the <b>Wide</b> rule breadth. You cannot change this setting.</li> <li>■ <b>Optional Validators</b>                      Custom data identifiers support all optional validators, but they are configured at the policy instance level.</li> </ul>

## Manage and add 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 [“About data identifiers”](#) on page 416.

**Table 20-17** Manage data identifiers

Action	Description
Edit a data identifier.	Select the data identifier from the list to modify it. See <a href="#">“Selecting system data identifier breadth”</a> on page 436. See <a href="#">“About modifying data identifiers”</a> on page 425. See <a href="#">“Modifying and creating data identifiers”</a> on page 441.

**Table 20-17** Manage data identifiers (*continued*)

Action	Description
Define a custom data identifier.	Click <b>Add Data Identifier</b> to create a custom data identifier. See <a href="#">“About custom data identifiers”</a> on page 429. See <a href="#">“Implementing custom data identifiers”</a> on page 443.
Sort and view data identifiers.	The list is sorted alphabetical by <b>Name</b> . 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 identifier.	Click the X icon on the right side to delete a data identifier. The system does not let you delete system data identifiers. You can only delete custom data identifiers.

## Configuring the Content Matches Data Identifier condition

You can configure the Content Matches Data Identifier condition in policy detection rules and exceptions.

See [“About data identifiers”](#) on page 416.

**Table 20-18** Configuring the Content Matches Data Identifier condition

Step	Action	Description
Step 1	Add a data identifier rule or exception to a policy, or configure an existing one.	Select the <b>Content Matches Data Identifier</b> condition at the <b>Add Detection Rule</b> or <b>Add Exception</b> screen. See <a href="#">“Adding a rule to a policy”</a> on page 340. See <a href="#">“Adding an exception to a policy”</a> on page 349.
Step 2	Choose a data identifier.	Choose a data identifier from the list and click <b>Next</b> . See <a href="#">“Available system data identifiers”</a> on page 417.

**Table 20-18**      Configuring the Content Matches Data Identifier condition  
*(continued)*

Step	Action	Description
Step 3	Select a <b>Breadth</b> of detection.	<p>Use the breadth option to narrow the scope of detection.</p> <p>See <a href="#">“About data identifier breadths”</a> on page 420.</p> <p>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.</p> <p>See <a href="#">“Selecting system data identifier breadth”</a> on page 436.</p>
Step 4	Select and configure one or more <b>Optional Validators</b> .	<p>Optional validators restrict the match criteria and reduce false positives.</p> <p>See <a href="#">“About optional validators”</a> on page 421.</p>
Step 5	Configure <b>Match Counting</b> .	<p>Select how you want to count matches:</p> <ul style="list-style-type: none"> <li>■ <b>Check for existence</b> Do not count multiple matches; report a match count of 1 for one or more matches.</li> <li>■ <b>Count all matches</b> Count each match; specify the minimum number of matches to report an incident.</li> </ul> <p>See <a href="#">“Configuring match counting”</a> on page 346.</p>
Step 6	Configure the message components to <b>Match On</b> .	<p>Select one or more message components on which to match.</p> <p>On the endpoint, the detection engine matches the entire message, not individual components.</p> <p>See <a href="#">“Selecting components to match on”</a> on page 348.</p> <p>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.</p> <p>See <a href="#">“About cross-component matching for data identifiers”</a> on page 425.</p>
Step 7	Configure additional conditions to <b>Also Match</b> .	<p>Optionally, you can <b>Add</b> one or more additional conditions from any available in the <b>Also Match</b> condition list.</p> <p>All conditions in a compound rule or exception must match to trigger or except an incident.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

# Selecting system data identifier breadth

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 420.

---

**Note:** 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 422.

---

**Table 20-19** System data identifier breadths and normalizers

Data Identifier	Breadth(s)	Normalizer
ABA Routing Number See <a href="#">“ABA Routing Number system data identifier”</a> on page 536.	Wide Medium Narrow	Digits Only
Australian Medicare Number See <a href="#">“Australian Medicare Number system data identifier”</a> on page 539.	Wide	Digits Only
Australian Tax File Number See <a href="#">“Australian Tax File Number system data identifier”</a> on page 540.	Wide	Digits Only
Burgerservicenummer See <a href="#">“Burgerservicenummer system data identifier”</a> on page 540.	Wide	Digits Only
Canadian Social Insurance Number See <a href="#">“Canadian Social Insurance Number system data identifier”</a> on page 541.	Wide Medium Narrow	Digits Only
Codice Fiscale See <a href="#">“Codice Fiscale system data identifier”</a> on page 543.	Wide	Digits Letters Only

**Table 20-19** System data identifier breadths and normalizers (*continued*)

Data Identifier	Breadth(s)	Normalizer
Credit Card Magnetic Stripe Data See “ <a href="#">Credit Card Magnetic Stripe Data system data identifier</a> ” on page 544.	Medium	Digits Only
Credit Card Number See “ <a href="#">Credit Card Number system data identifier</a> ” on page 546.	Wide Medium Narrow	Digits Only
CUSIP Number See “ <a href="#">CUSIP Number system data identifier</a> ” on page 552.	Wide Medium Narrow	Lowercase
Driver's License Number – CA State See “ <a href="#">Drivers License Number – CA State system data identifier</a> ” on page 554.	Wide Medium	Lowercase
Driver's License Number – FL, MI, MN States See “ <a href="#">Drivers License Number - FL, MI, MN States system data identifier</a> ” on page 556.	Wide Medium	Lowercase
Driver's License Number – IL State See “ <a href="#">Drivers License Number - IL State system data identifier</a> ” on page 557.	Wide Medium	Lowercase
Driver's License Number – NJ State See “ <a href="#">Drivers License Number - NJ State system data identifier</a> ” on page 559.	Wide Medium	Lowercase
Driver's License Number – NY State See “ <a href="#">Drivers License Number - NY State system data identifier</a> ” on page 560.	Wide Medium	Lowercase
French INSEE Code See “ <a href="#">French INSEE Code system data identifier</a> ” on page 562.	Wide	Digits Only
Hong Kong ID See “ <a href="#">Hong Kong ID system data identifier</a> ” on page 562.	Wide	Lowercase

**Table 20-19** System data identifier breadths and normalizers (*continued*)

Data Identifier	Breadth(s)	Normalizer
IBAN Central See <a href="#">“IBAN Central system data identifier”</a> on page 563.	Wide	None
IBAN East See <a href="#">“IBAN East system data identifier”</a> on page 565.	Wide	None
IBAN West See <a href="#">“IBAN West system data identifier”</a> on page 568.	Wide	None
IP Address See <a href="#">“IP Address system data identifier”</a> on page 570.	Wide Medium Narrow	None
National Drug Code See <a href="#">“National Drug Code (NDC) system data identifier”</a> on page 572.	Wide Medium Narrow	None
People's Republic of China ID See <a href="#">“People's Republic of China ID system data identifier”</a> on page 575.	Wide	Lowercase
Singapore NRIC See <a href="#">“Singapore NRIC system data identifier”</a> on page 575.	Wide	Lowercase
South Korean Resident Registration Number See <a href="#">“South Korea Resident Registration Number system data identifier”</a> on page 576.	Wide Medium	Digits Only
Spanish DNI ID See <a href="#">“Spanish DNI ID system data identifier”</a> on page 577.	Wide	Lowercase
SWIFT Code See <a href="#">“SWIFT Code system data identifier”</a> on page 578.	Wide Narrow	Swift

**Table 20-19** System data identifier breadths and normalizers (*continued*)

Data Identifier	Breadth(s)	Normalizer
Swiss AHV Number See “ <a href="#">Swiss AHV Number system data identifier</a> ” on page 580.	Wide	Digits Only
Taiwan ROC ID See “ <a href="#">Taiwan ROC ID system data identifier</a> ” on page 580.	Wide	None
UK Driver's License Number See “ <a href="#">UK Drivers License Number system data identifier</a> ” on page 581.	Wide Medium	Lowercase
UK Electoral Roll Number See “ <a href="#">UK Electoral Roll Number system data identifier</a> ” on page 583.	Wide	Lowercase
UK National Health Service (NHS) Number See “ <a href="#">UK National Health Service (NHS) Number system data identifier</a> ” on page 584.	Medium Narrow	Digits Only
UK National Insurance Number See “ <a href="#">UK National Insurance Number system data identifier</a> ” on page 586.	Wide Medium Narrow	Lowercase
UK Passport Number See “ <a href="#">UK Passport Number system data identifier</a> ” on page 589.	Wide Medium Narrow	None
UK Tax ID Number See “ <a href="#">UK Tax ID Number system data identifier</a> ” on page 591.	Wide Medium Narrow	None
US Individual Tax ID Number (ITIN) See “ <a href="#">US Individual Tax Identification Number (ITIN) system data identifier</a> ” on page 593.	Wide Medium Narrow	Digits Only

**Table 20-19** System data identifier breadths and normalizers (*continued*)

Data Identifier	Breadth(s)	Normalizer
US Social Security Number (SSN) See <a href="#">"US Social Security Number (SSN) system data identifier"</a> on page 596.	Wide Medium Narrow	Digits Only

## 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"](#) on page 421.

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 20-10](#) on page 423.

### 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 434.
- 2 Select one or more optional validators.  
See ["About optional validators"](#) on page 421.
- 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 20-10](#) on page 423.

# Modifying and creating data identifiers

You can modify and create 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 [“About modifying data identifiers”](#) on page 425.

**Table 20-20** Modifying and creating system data identifiers

Step	Action	Description
Step 1	Create a custom data identifier, or modify an existing one.	See <a href="#">“Implementing custom data identifiers”</a> on page 443. If you modify a system data identifier, click the plus sign to display the breadth and edit the data identifier. See <a href="#">“Selecting system data identifier breadth”</a> on page 436.
Step 2	Supply or edit one or more <b>Patterns</b> .	You can modify any pattern that the data identifier provides. See <a href="#">“Implementing patterns to match data”</a> on page 444.
Step 3	Edit the data input for any validator that accepts input.	See <a href="#">“Editing required validator input”</a> on page 442.
Step 4	Add or remove <b>Validators</b> , as necessary.	See <a href="#">“Selecting required data validators”</a> on page 445.
Step 5	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 <a href="#">“Manage and add data identifiers”</a> on page 433. <b>Note:</b> Click <b>Cancel</b> to not save the data identifier.
Step 6	Implement the data identifier in a policy rule or exception.	See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.

## Manually cloning a system data identifier before modifying it

The Enforce Server does not provide an automated mechanism for cloning a system data identifier.

See [“About modifying data identifiers”](#) on page 425.

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

- 1 Review the original configuration of the data identifier you want to modify.
- 2 Create a custom data identifier.  
See [“Implementing custom data identifiers”](#) on page 443.
- 3 Copy the configuration of the original data identifier to the custom data identifier.  
Add the pattern(s), validator(s), any data input, and the normalizer.  
See [“Selecting system data identifier breadth”](#) on page 436.
- 4 Save the custom data identifier.
- 5 Modify the custom data identifier to suit your needs.

## Editing required 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 validators”](#) on page 426.

### To edit required validator input

- 1 Edit the data identifier by selecting it from the **Manage > Policies > Data Identifiers** screen.
- 2 Select the **Rule Breadth** you want to modify.  
Generally, the medium and narrow breadth options include validators that accept data input.

- 3 Select the validator from the **Active Validators** list whose input you want to edit.  
 For example, select **Find keywords**.
- 4 Edit the input for the validator in the **Description and Data Entry** field.
- 5 Click **Update Validator** to save the changes you have made to the validator input.  
 Click **Discard Changes** to not save the changes.
- 6 Click **Save** to save the data identifier.

## Implementing 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 [“About custom data identifiers”](#) on page 429.

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.

**Table 20-21** Implementing custom data identifiers

Step	Action	Description
Step 1	Select <b>Manage &gt; Policies &gt; Data Identifiers</b> .	The <b>Data Identifiers</b> screen lists all data identifiers available in the system.
Step 2	Select <b>Add Data Identifier</b> .	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.
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 <a href="#">“Implementing patterns to match data”</a> on page 444.

**Table 20-21** Implementing custom data identifiers (*continued*)

Step	Action	Description
Step 4	Select a <b>Data Normalizer</b> .	<p>You must select a data normalizer.</p> <p>The following normalizers are available:</p> <ul style="list-style-type: none"> <li>■ Digits</li> <li>■ Digits and Letters</li> <li>■ Lowercase</li> <li>■ Swift codes</li> <li>■ Do nothing</li> </ul> <p>Select this option if you do not want to normalize the data.</p> <p>See <a href="#">“About data normalizers”</a> on page 430.</p>
Step 5	Select zero or more <b>Validators</b> .	<p>Including a validator to check and verify pattern matching is optional.</p> <p>See <a href="#">“Selecting required data validators”</a> on page 445.</p>
Step 6	<b>Save</b> the custom data identifier.	<p>Click <b>Save</b> at the upper left of the screen.</p> <p>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.</p> <p>To edit a custom data identifier, select it from the list.</p> <p>See <a href="#">“Modifying and creating data identifiers”</a> on page 441.</p> <p><b>Note:</b> Click <b>Cancel</b> to not save the custom data identifier.</p>
Step 7	Implement the custom data identifier in one or more policies.	<p>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 - Add Rule</b> and the <b>Configure Policy - Add Exception</b> screens.</p> <p>See <a href="#">“Configuring the Content Matches Data Identifier condition”</a> on page 434.</p> <p>You can configure optional validators at the policy instance level for custom data identifiers.</p> <p>See <a href="#">“Configuring optional validators”</a> on page 440.</p>

## Implementing 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.

Patterns are defined using a syntax that is similar to regular expressions. However, much of the regex syntax is not supported.

See [“About data identifier patterns”](#) on page 426.

---

**Note:** The system only allows the use of ASCII characters for data identifier patterns.

---

#### To edit or implement a pattern

- 1 Review the patterns for the data identifier you want to modify.  
See [“Selecting system data identifier breadth”](#) on page 436.
- 2 Consider cloning the data identifier, if you are modifying a system data identifier.  
See [“Manually cloning a system data identifier before modifying it”](#) on page 442.
- 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.  
Patterns are implemented as regular expressions. Patterns are delimited by line breaks.  
See [“About writing regular expressions”](#) on page 459.
- 7 Click **Save** to save the data identifier.

## Selecting required data validators

Symantec Data Loss Prevention provides a comprehensive set of validators to facilitate pattern matching accuracy.

See [“About validators”](#) on page 426.

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 required data validators](#)" on page 445.

#### To select a pattern validator

- 1 Create a custom data identifier.  
See "[Implementing custom data identifiers](#)" on page 443.
- 2 In the **Validators** section, select the desired validator.  
See "[About validators](#)" on page 426.
- 3 If the validator does not require data input, click **Add Validator**.  
The validator is added to the **Active Validators** list.
- 4 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.
- 6 Click **Save** to save the configuration of the data identifier.

## Implementing 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 Customization Guide* for details on using the Symantec Data Loss Prevention Scripting Language.

---

### To implement a custom script validator

- 1 Modify an existing data identifier or create a custom data identifier.  
See [“Implementing custom data identifiers”](#) on page 443.
- 2 Select the **Custom Script** validator from the list of **Validation Checks**.
- 3 Enter your custom script in the **Description and Data Entry** field.
- 4 Click **Add Validator** to add the custom validator to the **Active Validators** list.
- 5 Click **Save** to save the configuration of the data identifier.

## Data identifier best practices

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. False positives occur when a detection rule detects content that is not a violation. False negatives occur when a detection rule does not detect content but the content is a violation. Proper configuration of data identifiers to match content requires a proper balance between false negatives and false positives.

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.

Sometimes, to reduce false positives, it may be useful to not match on the “Envelope” message component. Information contained in the message header for HTTP transmissions contain session IDs which can trigger a false data identifier match. For example, some social media sites such as Facebook and LinkedIn contain a session ID that may at times match CCN/SSNs exactly.

See [“About achieving precise detection results”](#) on page 301.

Before you modify a system data identifier or create a custom one, consider the following best practices:

- If you want to modify a system data identifier, clone it as a custom data identifier and then modify the cloned copy.
- Data identifiers do not export as part of a policy template.  
An exported template contains a reference to each data identifier implemented in that policy. On import to a target system, the template uses the identifier reference to select the local data identifier. If the system data identifier is modified, on import it cannot be recognized by the target system.  
You can also add the data identifier to a policy and export the policy as a template before modifying the data identifier. The best practice is to refer to

the documentation for the system data identifier, then manually clone it as a custom data identifier and then modify the cloned version. In this fashion you preserve the state of the original system data identifier.

# Detecting content using keyword matching

This chapter includes the following topics:

- [About implementing keyword matching](#)
- [About keyword proximity matching](#)
- [Keyword matching examples](#)
- [Configuring the Content Matches Keyword condition](#)
- [About profiling keyword dictionaries](#)
- [Keyword matching best practices](#)

## About implementing keyword matching

Symantec Data Loss Prevention provides keyword matching detection. Keyword matching uses a list of one or more keywords or phrases to detect data loss. The detection engine checks message components against each keyword in the list for matches.

**Table 21-1** Implementing keyword matching

Keyword matching features	Description
Match on whole or partial keywords and key phrases.	Separate each keyword or phrase by a newline or comma. See <a href="#">“Keyword matching examples”</a> on page 451.

**Table 21-1** Implementing keyword matching (*continued*)

Keyword matching features	Description
Match on the wildcard asterisk (*) character.	Match the wildcard at the end of a keyword, in whole word mode only.  See <a href="#">“Keyword matching examples”</a> on page 451.
Keyword proximity matching.	Match across a range of keywords.  See <a href="#">“About keyword proximity matching”</a> on page 450.
Find keywords.	Implement one or more keywords in data identifiers to refine the scope of detection.  See <a href="#">“About data identifiers”</a> on page 416.
Policy rules and exceptions.	You can implement keyword matching in policy rules and exceptions.  See <a href="#">“Configuring the Content Matches Keyword condition”</a> on page 452.
Cross-component matching.	Keyword matching detects on one or more message components.  See <a href="#">“About message components that can be matched”</a> on page 293.
Keyword dictionary.	If you have a large dictionary of keywords, you can create an Exact Data Profile and index the keyword list.  See <a href="#">“About profiling keyword dictionaries”</a> on page 455.

## About keyword proximity matching

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 rule 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” rule as a detection exception. In this case any occurrence of the words “confidential” and “information” within 10 words of each is excepted from matching.

---

**Note:** The word distance (proximity value) is exclusive of detected keywords. Thus, a word distance of 10 allows for a proximity window of 12 words.

---

See “[Keyword matching examples](#)” on page 451.

See “[Configuring the Content Matches Keyword condition](#)” on page 452.

## 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).

**Table 21-2** Keyword matching examples

Keyword type	Keyword(s)		Matches	Does Not Match
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	Newline delimited:	Comma delimited:	hacks hack	hackers shack
	hack hacker hacks	hack, hacker, hacks	hacker	

**Table 21-2** Keyword matching examples (*continued*)

Keyword type	Keyword(s)	Matches	Does Not Match
keyword with wildcard	priv*	private privilege privy privity privs	prize prevent 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, enrout, 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

See [“Keyword matching best practices”](#) on page 456.

## Configuring the Content Matches Keyword condition

The Content Matches Keyword detection rule lets you match content using keywords and key phrases.

See [“About implementing keyword matching”](#) on page 449.

You can implement keyword matching conditions in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

**To configure the Content Matches Keyword condition**

- 1 Add a new keyword condition to a policy rule or exception, or modify an existing one.  
 See [“Configuring policy rules”](#) on page 342.  
 See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the keyword matching parameters.  
 See [Table 21-3](#) on page 453.
- 3 Save the policy.

**Table 21-3** Configure the Content Matches Keyword condition

Action	Description
Enter the match type.	Select if you want the keyword match to be: <b>Case Sensitive</b> or <b>Case Insensitive</b> Case insensitive is the default.
Choose the keyword separator.	Select the keyword separator you to delimit multiple keywords: <b>Newline</b> or <b>Comma</b> . 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 <a href="#">“Keyword matching examples ”</a> on page 451.

**Table 21-3** Configure the Content Matches Keyword condition (*continued*)

Action	Description
Configure keyword proximity matching (optional).	<p>Keyword proximity matching lets you specify a range of detection among keyword pairs.</p> <p>See <a href="#">“About keyword proximity matching”</a> on page 450.</p> <p>To implement keyword proximity matching:</p> <ul style="list-style-type: none"> <li>■ Select (check) the <b>Keyword Proximity matching</b> option in the “Conditions” section of the rule builder interface.</li> <li>■ Click <b>Add Pair of Keywords</b>.</li> <li>■ Enter a pair of keywords.</li> <li>■ Specify the <b>Word distance</b>.</li> </ul> <p>The maximum distance between keywords is 999, as limited by the three-digit length of the “Word distance” field. The word distance is exclusive of detected keywords. For example, a word distance of <b>10</b> allows for a range of 12 words, including the two words comprising the keyword pair.</p> <ul style="list-style-type: none"> <li>■ Repeat the process to add additional keyword pairs.</li> </ul> <p>The system connects multiple keyword pair entries the OR Boolean operator, meaning that the detection engine evaluates each keyword pair independently.</p>
Match on whole or partial keywords.	<p>Select the option <b>On whole words only</b> to match on whole keywords only.</p> <p>See <a href="#">“Keyword matching examples ”</a> on page 451.</p> <p><b>Note:</b> You must match on whole words only if you use the asterisk (*) wildcard character in any keyword you enter in the list.</p>
Configure match conditions.	<p>Keyword matching lets you specify how you want to count condition matches.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Check for existence</b> The system reports one incident for all matches.</li> <li>■ <b>Count all matches</b> The system reports one incident for each match (default setting).</li> <li>■ <b>only report incidents with at least _ matches</b> The system reports each match once the match threshold you specify is met.</li> </ul> <p>See <a href="#">“Configuring match counting”</a> on page 346.</p>

**Table 21-3** Configure the Content Matches Keyword condition (*continued*)

Action	Description
Select components to match on.	<p>Keyword matching detection supports matching across message components.</p> <p>See <a href="#">“Selecting components to match on”</a> on page 348.</p> <p>Select one or more message components to match on:</p> <ul style="list-style-type: none"> <li>■ <b>Envelope</b> – Header metadata used to transport the message</li> <li>■ <b>Subject</b> – Email subject of the message (only applies to SMTP)</li> <li>■ <b>Body</b> – The content of the message</li> <li>■ <b>Attachments</b> – Any files attached to or transferred by the message</li> </ul> <p><b>Note:</b> On the endpoint the DLP Agent matches on the entire message, not individual components.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p>
Also match one or more additional conditions.	<p>Select this option to create a compound condition. All conditions must be met to report a match.</p> <p>You can <b>Add</b> any available condition from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

See [“Keyword matching best practices”](#) on page 456.

## About profiling 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. In this case you create a file containing all the keywords you want to protect, each on a separate line (like a single-column table). You then create an Exact Data Profile based on the keyword data source file. When you define a policy, you select the profile to protect the data that matches your defined keywords.

When you add an EDM rule based on a keyword dictionary, the detection engine excludes many common words across various languages. If you use a keyword list and want to detect common words, remove them from the corresponding file in the `Vontu_Home\Protect\config\stopwords` directory. Alternatively you can use a keyword, pattern, or regular expression rule instead of the EDM rule.

See [“About implementing Exact Data Matching”](#) on page 368.

## Keyword matching best practices

When you implement keyword matching detection, consider the following:

- Symantec Data Loss Prevention checks input content for every keyword in a condition.
- Do not use quotation marks when you enter key phrases. The quotes are interpreted literally. (That is, they are required in the match.)
- White space before and after keywords or key phrases is stripped out.
- The case sensitivity option you choose applies to all keywords in the list for that condition.
- With match on whole words only enabled (which is the default), keywords match at word boundaries only (\W for those familiar with regular expressions). Any characters other than A-Z, a-z, and 0-9 are interpreted as word boundaries.
- With match on whole words only enabled (which is the default), 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.
- Plurals and verb inflections must be enumerated. If the number of enumerations becomes complicated, consider using a regular expression rule.
- You can enter key phrases, such as "social security number" (without the quotes). Symantec Data Loss Prevention looks for the entire phrase without returning matches on individual constituent words (such as social or security).
- The system only detects the exact keyword, not variants. For example, if you specify key phrase "social security number," the detection engine does not match a phrase that contains two spaces between the words.
- The system implies an OR between keywords. That is, content matches if it contains any of the keywords, not necessarily all of them. To perform an ALL (or AND) match, combine multiple keyword conditions in a compound rule or exception.
- To match all of a large number of keywords (keyword dictionary), use an Exact Data Profile.

See [“About implementing keyword matching”](#) on page 449.

# Detecting content using regular expressions

This chapter includes the following topics:

- [About regular expression matching](#)
- [Configuring the Content Matches Regular Expression condition](#)
- [About writing regular expressions](#)
- [Regular expression detection best practices](#)

## About regular expression matching

Regular expressions provide a mechanism for identifying strings of text, such as particular characters, words, or patterns of characters.

The Content Matches Regular Expression detection method 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.

See [“Configuring the Content Matches Regular Expression condition”](#) on page 457.

See [“Regular expression detection best practices”](#) on page 460.

## Configuring the Content Matches Regular Expression condition

The Content Matches Regular Expression detection condition lets you detect and except message content using regular expressions.

See [“About regular expression matching”](#) on page 457.

You can implement this condition in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

**To configure a Content Matches Regular Expression condition**

- 1 Add a Content Matches Regular Expression condition to a policy, or edit an existing one.  
 See [“Configuring policy rules”](#) on page 342.  
 See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the Content Matches Regular Expression condition parameters.  
 See [Table 22-1](#) on page 458.
- 3 Save the policy configuration.

**Table 22-1** Content Matches Regular Expression parameters

Action	Description
Match regex.	Specify a regular expression to be matched. See <a href="#">“About writing regular expressions”</a> on page 459.
Configure match counting.	Configure how you want to count matches. See <a href="#">“Configuring match counting”</a> on page 346.  <b>Check for existence</b> 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.
Match on one or more message components.	Configure cross-component matching by selecting one or more message components to match on. <ul style="list-style-type: none"> <li>■ <b>Envelope</b> – The header of the message, transport metadata.</li> <li>■ <b>Subject</b> – The email subject (only applies to email messages).</li> <li>■ <b>Body</b> – The content of the message.</li> <li>■ <b>Attachments</b> – The content of any files that are attached to or transported by the message.</li> </ul> See <a href="#">“Selecting components to match on”</a> on page 348.  <b>Note:</b> On the endpoint the DLP Agent matches the entire message regardless of any individually selected components. See <a href="#">“About message components that can be matched”</a> on page 293.

**Table 22-1** Content Matches Regular Expression parameters (*continued*)

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 available condition from the list.  See <a href="#">“Configuring compound match conditions”</a> on page 354.

## About writing regular expressions

Although there is no substitute for a good regular expression tutorial, the following provides some reference constructs for character matching.

**Table 22-2** Regular expression constructs

Regex construct	Description
.	Any single character (except for newline characters)
\d	Any digit (0–9)
\s	Any white space
\w	Any word character (a–z, A–Z, 0–9, _)
\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.)

**Table 22-2** Regular expression constructs (*continued*)

Regex construct	Description
(?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
	Means OR (For example, A B means regular expression A or regular expression B.)

See [“About regular expression matching”](#) on page 457.

## Regular expression detection best practices

Consider using Data Identifiers before implementing regular expression detection. Data Identifiers are more efficient because their patterns are precisely tuned for accuracy. For example, if you want to search for social security numbers, use the US Social Security Number (SSN) Data Identifier instead of a regex.

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.

See [“About regular expression matching”](#) on page 457.

Symantec Data Loss Prevention implements a significant enhancement to improve the performance of regular expressions. To achieve the improved performance, the look ahead and look behind sections must exactly match one of the supported standard sections.

The following table 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.

**Table 22-3** Look ahead and look behind standard sections

Operation	Construct
Look ahead	(?= (?: [^-\w] )   \$)

**Table 22-3** Look ahead and look behind standard sections (*continued*)

Operation	Construct
Look behind	<pre>(?&lt;=(^ (?:[^\d][^\w+])))) and (?&lt;=(^ (?:[^\d][^\w+]) \t))</pre>

See [“About writing regular expressions”](#) on page 459.



# Detecting file properties

This chapter includes the following topics:

- [About implementing file property matching](#)
- [About file type detection](#)
- [Detectable file types](#)
- [About custom file type detection](#)
- [About file size detection](#)
- [About file name detection](#)
- [File name detection examples](#)
- [Configuring the Message Attachment or File Type Match condition](#)
- [Configuring the Message Attachment or File Size Match condition](#)
- [Configuring the Message Attachment or File Name Match condition](#)
- [Enabling custom file type detection](#)
- [Configuring the Custom File Type Signature condition](#)
- [File property detection best practices](#)

## About implementing file property matching

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 methods to except files and attachments from detection based on their context.

**Table 23-1** File Properties detection conditions

Detection condition	Description
Message Attachment or File Type Match	Detect or except specific files and attachments by type. See <a href="#">“About file type detection”</a> on page 464. See <a href="#">“Configuring the Message Attachment or File Type Match condition”</a> on page 481.
Message Attachment or File Size Match	Detect or except specific files and attachments by size. See <a href="#">“About file size detection”</a> on page 480. See <a href="#">“Configuring the Message Attachment or File Size Match condition”</a> on page 482.
Message Attachment or File Name Match	Detect or except specific files and attachments by name. See <a href="#">“About file name detection”</a> on page 480. See <a href="#">“Configuring the Message Attachment or File Name Match condition”</a> on page 483.
Custom File Type Signature	Detect or except custom file types.

## About file type detection

Symantec Data Loss Prevention can recognize over 330 file types.

See [“About file types that can be detected”](#) on page 282.

The detection engine does not rely on the file extension to match. For example, say a user changes the .mp3 file name extension to .doc and emails the file. The detection engine looks at the binary signature of the file to determine that it is an MP3 file, regardless of the file name extension.

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.

Refer to the associated topic for configuration details.

See [“Configuring the Message Attachment or File Type Match condition”](#) on page 481.

# Detectable file types

Symantec Data Loss Prevention can recognize over 330 file types.

**Note:** The content of these files is not scanned, only the file type is recognized. See “[Detectable content types](#)” on page 395.

**Table 23-2** File types that can be recognized

Recognizable file types
7-Zip Compressed File (7Z)
Ability Office (SS)
Ability Office (DB)
Ability Office (GR)
Ability Office (WP)
Ability Office (COM)
ACT
Adobe FrameMaker
Adobe FrameMaker Interchange Format
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
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
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)
CADAM Drawing Overlay
CATIA Drawing (CAT)
CCITT Group 3 1-Dimensional (G31D)
COMET TOP Word
Comma Separated Values

**Table 23-2** File types that can be recognized (*continued*)

Recognizable file types
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)
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

**Table 23-2** File types that can be recognized (*continued*)

Recognizable file types
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
EBCDIC Text
EMC EmailXtender Container File (EMX)
ENABLE
ENABLE Spreadsheet (SSF)
Encapsulated PostScript (raster)
Enhanced Metafile
Envoy (EVY)
Executable- Other
Executable- UNIX
Executable- VAX
Executable- SUN
FileMaker (Macintosh)
Folio Flat File
Framework

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
Framework II
FTP Session Data
Fujitsu Oasys
GEM Bit Image
GIF
Graphics Environment Manager (GEM VDI)
GZIP
Haansoft Hangul
Harvard Graphics
Hewlett-Packard
Honey Bull DSA101
HP Graphics Language (HPG)
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
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
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
Lotus SmartMaster
Lotus Word Pro
Lyrix MacBinary
MacBinary
Macintosh Raster
MacPaint
Macromedia Director
Macromedia Flash
MacWrite
MacWrite II
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 Outlook Personal Folder
Microsoft Outlook

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
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 PowerPoint Windows Macro-Enabled 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 Icon (ICO)
Microsoft Windows OLE 2 Encapsulation
Microsoft Windows Write
Microsoft Word (UNIX)
Microsoft Word Macintosh
Microsoft Word PC
Microsoft Word Windows

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
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 Works Database (PC)
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
NBI Net Archive Format
Netscape Bookmark file
NeWS font file (SUN)
NeXT/Sun Audio
NIOS TOP
Nota Bene
Nurestor Drawing (NUR)
Oasis Open Document Format (ODT)
Oasis Open Document Format (ODS)
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)

**Table 23-2** File types that can be recognized (*continued*)

Recognizable file types
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
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)

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
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)
Quark Express (Macintosh)
QuickDraw 3D Metafile (3DMF)
QuickTime Movie
RAR archive
Real Audio
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
StarOffice Calc (SXC)
StarOffice Calc (ODS)
StarOffice Impress (SXI)
StarOffice Impress (SXP)
StarOffice Impress (ODP)
StarOffice Writer (SXW)
StarOffice Writer (ODT)
Stuff It Archive (Macintosh)
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

**Table 23-2** File types that can be recognized (*continued*)

<b>Recognizable file types</b>
Usenet format
UUEncoding
Volkswriter
VRML
Wang Office GDL Header Encapsulation
WANG PC
Wang WITA
WANG WPS Comm.
Windows Animated Cursor
Windows Bitmap
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

**Table 23-2** File types that can be recognized (*continued*)

Recognizable file types
WordPerfect Graphics 1
WordPerfect Graphics 2
WordStar
WordStar 2000
WordStar 6.0
WriteNow
Writing Assistant word processor
X Bitmap (XBM)
X Image
X Pixmap (XPM)
Xerox 860 Comm.
Xerox Writer word processor
XHTML
XML (generic)
XML Paper Specification
XyWrite

## About custom file type detection

If the type of file you want to detect is not supported as a system default filetype, Symantec Data Loss Prevention provides you with the ability to detect custom file types using scripts.

See [“About file types that can be detected”](#) on page 282.

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. Custom file type detection is disabled by default. To implement this detection method you need to enable it in the Enforce Server.

See [“Configuring the Custom File Type Signature condition”](#) on page 485.

See the *Symantec Data Loss Prevention Detection Customization Guide* for details on writing custom file type scripts.

## About file size detection

Symantec Data Loss Prevention provides message attachment and file size matching. Detection is based on either or both of the body or attachment message components, 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 [“Configuring the Message Attachment or File Size Match condition”](#) on page 482.

## About file name detection

Symantec Data Loss Prevention provides message attachment and file name matching. This method of detection is used to detect the names of files and attachments.

The detection engine supports the DOS pattern matching syntax to detect file names, including wildcards.

**Table 23-3** DOS Operators for file name detection

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.

See [Table 23-4](#) on page 481.

See [“Configuring the Message Attachment or File Name Match condition”](#) on page 483.

## File name detection examples

The following DOS pattern matching expressions are provided as examples for configuring the Message Attachment or File Name condition.

**Table 23-4** 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.

## Configuring the Message Attachment or File Type Match condition

The Message Attachment or File Type Match detection condition matches or excepts the file type of an attachment message component.

See [“About file type detection”](#) on page 464.

You can configure an instance of this condition in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

### To configure the Message Attachment or File Type Match condition

- 1 Add a Message Attachment or File Type Match condition to a policy rule or exception, or edit an existing one.  
 See [“Configuring policy rules”](#) on page 342.  
 See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the Message Attachment or File Type Match condition parameters.  
 See [Table 23-5](#) on page 482.
- 3 Click **Save** to save the policy.

**Table 23-5** Message Attachment or File Type Match detection rule

Action	Description
Select the file types.	<p>Select all of the formats you want to match.</p> <p>See <a href="#">“Detectable file types”</a> on page 465.</p> <p>Click <b>select all</b> or <b>deselect all</b> to select or deselect all formats.</p> <p>To select all formats within a certain category (for example, all word-processing formats), click the section heading.</p> <p>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.</p>
Match on attachments only.	<p>This condition only matches on the <b>Message Attachments</b> component.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p>
Also match on one or more additional conditions.	<p>Select this option to create a compound condition. All conditions must match to trigger or except an incident.</p> <p>You can <b>Add</b> any condition available from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

## 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.

See [“About file size detection”](#) on page 480.

You can configure an instance of this condition in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

**To configure the Message Attachment or File Size Match condition**

- 1 Add a Message Attachment or File Size Match condition to a policy, or edit an existing one.  
See [“Configuring policy rules”](#) on page 342.  
See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the Message Attachment or File Type Match condition parameters.  
See [Table 23-6](#) on page 483.
- 3 Click **Save** to save the policy.

**Table 23-6** Message Attachment or File Size Match parameters

Action	Description
Enter the Sizes.	<p>To specify the minimum size of attachments that you want to match, select <b>More Than</b>.</p> <p>To specify the maximum size of attachments that you want to match, select <b>Less Than</b>.</p> <p>Enter a number, and select the unit of measure: bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB).</p>
Match on the body or attachments.	<p>Select one or both of the following message components on which to base the match:</p> <ul style="list-style-type: none"> <li>■ <b>Body</b> – The content of the message.</li> <li>■ <b>Attachments</b> – Any files that are attached to or transferred by the message.</li> </ul> <p>See <a href="#">“Selecting components to match on”</a> on page 348.</p>
Also match one or more additional conditions.	<p>Select this option to create a compound condition. All conditions must match to trigger or except an incident.</p> <p>You can <b>Add</b> any condition available from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

## Configuring the Message Attachment or File Name Match condition

The Message Attachment or File Name Match detection condition detects or excepts messages based on the name of a file attached to the message.

See [“About file name detection”](#) on page 480.

You can configure an instance of this condition in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

**To configure the Message Attachment or File Name Match condition**

- 1 Add a Message Attachment or File Name Match condition to a policy, or edit an existing one.

See [“Configuring policy rules”](#) on page 342.

See [“Configuring policy exceptions”](#) on page 351.

- 2 Configure the Message Attachment or File Type Match condition parameters.

See [Table 23-7](#) on page 484.

- 3 Click **Save** to save the policy.

**Table 23-7** Message Attachment or File Name Match parameters

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 <a href="#">“File name detection examples”</a> on page 481. See <a href="#">“Configuring policy rules”</a> on page 342.
Match on attachments.	This condition only matches on the <b>Message Attachments</b> component. See <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

## Enabling custom file type detection

The custom file type policy rule is not enabled by default. To implement the Custom File Type Signature condition, you must first enable it.

See [“About custom file type detection”](#) on page 479.

**To enable the Custom File Type Signature rule**

- 1 Using a text editor, open the file  
`C:\Vontu\Protect\config\Manager.properties`
- 2 Set the following option to "true":  
`com.vontu.manager.policy.showcustomscriptrule=true`
- 3 Stop and then restart the Vontu Manager service.
- 4 Log back on to the Enforce Server Administration Console and add a new blank policy.
- 5 Add a new detection rule or exception and beneath the File Properties heading you see the **Custom File Type Signature** condition.
- 6 Configure the condition with your custom script.  
 See [“Configuring the Custom File Type Signature condition”](#) on page 485.

## Configuring the Custom File Type Signature condition

The Custom File Type Signature condition matches custom file types that you have scripted.

See [“About custom file type detection”](#) on page 479.

You can implement the Custom File Type signature condition in policy rules and exceptions.

See [“Configuring policies”](#) on page 338.

**To configure a Custom File Type Signature condition**

- 1 Add a Custom File Type Signature condition to a policy rule or exception, or edit an existing one.  
 See [“Configuring policy rules”](#) on page 342.  
 See [“Configuring policy exceptions”](#) on page 351.
- 2 Configure the Custom File Type Signature condition parameters.  
 See [Table 23-8](#) on page 485.
- 3 Click **Save** to save the policy.

**Table 23-8** Custom File Type Signature parameters

Action	Description
Enter the Script Name.	Specify the name of the script. The name must be unique across policies.

**Table 23-8** Custom File Type Signature parameters (*continued*)

Action	Description
Enter the scripted file type.	Enter the File Type Matches Signature script for detecting the binary signature of the custom file type.  Refer to the <i>Symantec Data Loss Prevention Detection Customization Guide</i> for details on writing custom scripts.
Match only on attachments.	This condition only matches on the <b>Message Attachments</b> component. See <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

## File property detection best practices

Keep in mind the following considerations when you implement file property detection:

- 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.
- The file size method counts both the body and any attachments in the file size you specify.

# Detecting network incidents

This chapter includes the following topics:

- [About network protocol matching](#)
- [Configuring Protocol Monitoring condition parameters](#)

## About network protocol matching

Symantec Data Loss Prevention provides the Protocol detection method which lets you detect network messages based on the communications transport method.

See “[Configuring Endpoint Monitoring condition parameters](#)” on page 493.

Symantec Data Loss Prevention supports detecting incidents on the primary Internet protocols, including the following:

- Email/SMTP
- HTTP
- HTTP/SSL
- IM:MSN
- IM:AIM
- IM:Yahoo
- FTP
- NNTP

In addition, you can add a custom protocol, such as a TCP tap on a specific port, to detect network incidents.

# Configuring Protocol Monitoring condition parameters

The Protocol or Endpoint Monitoring condition offers parameters for matching on network protocols.

You can implement an instance of the Protocol or Endpoint Monitoring condition in one or more policy detection rules and exceptions.

See [“Configuring policies”](#) on page 338.

**Table 24-1**      Configure Protocol Monitoring condition parameters

Action	Description
Add or modify the Protocol Monitoring condition.	Add a new <b>Protocol or Endpoint Monitoring</b> condition to a policy rule or exception, or modify an existing rule or exception condition. See <a href="#">“Configuring policy rules”</a> on page 342. See <a href="#">“Configuring policy exceptions”</a> on page 351.
Select one or more network protocols to match.	To detect Network incidents, select one or more <b>Network Protocols</b> . <ul style="list-style-type: none"> <li>■ Email/SMTP – Simple Mail Transfer Protocol, a protocol for sending email messages between servers.</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 data securely between a client and server.</li> <li>■ IM:MSN – MSN instant messaging , a type of communications service that enables you to create a private chat room with another individual.</li> <li>■ IM:AIM – AIM instant messaging.</li> <li>■ IM:Yahoo – Yahoo! Instant messaging.</li> <li>■ FTP – File Transfer Protocol is used on the Internet for transferring files from one computer to another.</li> <li>■ NNTP – Network News Transport Protocol is used to send, distribute, and retrieve USENET messages.</li> <li>■ TCP:custom_protocol – Transmission Control Protocol, user-defined TCP traffic.</li> </ul>
Configure endpoint monitoring.	See <a href="#">“Configuring Endpoint Monitoring condition parameters”</a> on page 493.

**Table 24-1**      Configure Protocol Monitoring condition parameters (*continued*)

Action	Description
Match on the entire message.	<p>The Protocol or Endpoint Monitoring condition matches on the entire message, not individual message components.</p> <p>The <b>Envelope</b> option is selected by default. You cannot select individual message components.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p>
Also match one or more additional conditions.	<p>Select this option to create a compound condition. All conditions must match to trigger or except an incident.</p> <p>You can <b>Add</b> any condition available from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>



# Detecting endpoint events

This chapter includes the following topics:

- [About implementing endpoint event detection](#)
- [About endpoint protocol, destination, and application detection](#)
- [About endpoint device detection](#)
- [About endpoint location detection](#)
- [Configuring Endpoint Monitoring condition parameters](#)
- [Gathering endpoint device IDs](#)
- [Manage and add endpoint devices](#)
- [Creating and modifying endpoint device configurations](#)
- [Configuring the Endpoint Device Class or ID condition](#)
- [Configuring the Endpoint Location condition](#)
- [Endpoint detection best practices](#)

## About implementing endpoint event detection

Endpoint detection matches events on endpoint computers where the Symantec DLP Agent is installed.

See [“About Endpoint Prevent monitoring”](#) on page 1052.

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 682.

**Table 25-1** Detecting endpoint events

Endpoint match conditions	Details
Endpoint Monitoring	Detect endpoint data based on the protocol, destination, or application.  See <a href="#">“About endpoint protocol, destination, and application detection”</a> on page 492.  See <a href="#">“Configuring Endpoint Monitoring condition parameters”</a> on page 493.
Endpoint Device or Class ID	Detect when users move endpoint data to a specific device.  See <a href="#">“About endpoint device detection”</a> on page 492.  See <a href="#">“Configuring the Endpoint Device Class or ID condition”</a> on page 498.
Endpoint Location	Detect when the endpoint is on or off the corporate network.  See <a href="#">“About endpoint location detection”</a> on page 493.  See <a href="#">“Configuring the Endpoint Location condition”</a> on page 499.

## About endpoint protocol, destination, and application detection

On the endpoint you can detect data loss based on the transport protocol, such as email (SMTP), Web (HTTP), and file transfer (FTP).

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.

You can create exceptions for allowable use scenarios.

See [“Configuring Endpoint Monitoring condition parameters”](#) on page 493.

## 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 496.

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 endpoint computers. 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 497.

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 498.

## 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 499.

## Configuring Endpoint Monitoring condition parameters

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.

See ["Configuring policies"](#) on page 338.

**Table 25-2** Configure the Endpoint Monitoring condition

Action	Description
Add or modify the Endpoint Monitoring condition.	Add a new <b>Protocol or Endpoint Monitoring</b> condition to a policy rule or exception, or modify an existing rule or exception condition. See <a href="#">“Configuring policy rules”</a> on page 342. See <a href="#">“Configuring policy exceptions”</a> on page 351.
Select one or more endpoint protocols to match.	To detect Endpoint incidents, select one or more <b>Endpoint Protocols</b> : <ul style="list-style-type: none"> <li>■ Email/SMTP – Simple Mail Transfer Protocol, a protocol for sending email messages between servers.</li> <li>■ HTTP – 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 data securely between a client and server.</li> <li>■ IM:MSN – MSN instant messaging , a type of communications service that enables you to create a private chat room with another individual.</li> <li>■ IM:AIM – AOL instant messaging.</li> <li>■ IM:Yahoo – Yahoo! Instant messaging.</li> <li>■ FTP – File Transfer Protocol is a common protocol that is used on the Internet for transferring files from one computer to another.</li> </ul>
Select one or more network protocols.	To detect Network incidents, select one or more <b>Network Protocols</b> . See <a href="#">“Configuring Protocol Monitoring condition parameters”</a> on page 488.

**Table 25-2**      Configure the Endpoint Monitoring condition (*continued*)

Action	Description
Select one or more endpoint destinations.	<p>To detect when users move data on the endpoint, select one or more <b>Endpoint Destinations</b>:</p> <ul style="list-style-type: none"> <li>■ Local Drive – Detect events on the local disk.</li> <li>■ CD/DVD – The CD/DVD burner on the endpoint computer. This destination can be any type of third-party CD/DVD burning software.</li> <li>■ Removable Storage Device – Detect data that is transferred to any USB or FireWire connected storage device.</li> <li>■ Copy to Network Share – Detect data that is transferred to any network share or remote file access.</li> <li>■ 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.</li> <li>■ Clipboard – The Windows Clipboard used to copy and paste data between Windows applications.</li> </ul>
Monitor endpoint applications.	<p>To detect when endpoint applications access files, select the <b>Application File Access</b> option.</p> <p>The DLP Agent monitors applications when they access sensitive files.</p> <p>See “<a href="#">About application monitoring</a>” on page 1131.</p> <p>The DLP Agent monitors any third-party application you add and configure at the <b>System &gt; Agents &gt; Application Monitoring</b> screen.</p> <p>See “<a href="#">Adding an application</a>” on page 1132.</p>
Match on the entire message.	<p>The DLP Agent evaluates the entire message, not individual message components.</p> <p>The <b>Envelope</b> option is selected by default. You cannot select the other message components.</p> <p>See “<a href="#">About message components that can be matched</a>” on page 293.</p>
Also match one or more additional conditions.	<p>Select this option to create a compound condition. All conditions must match to trigger or except an incident.</p> <p>You can <b>Add</b> any condition available from the list.</p> <p>See “<a href="#">Configuring compound match conditions</a>” on page 354.</p>

See “[About endpoint protocol, destination, and application detection](#)” on page 492.  
 See “[Endpoint detection best practices](#)” on page 500.

## 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 497.

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 1140.

---

**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.
- 5 Double-click the device instance. Or, right-click the device instance and select **Properties**.
- 6 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 497.

See [“About endpoint device detection”](#) on page 492.

See [“Manage and add endpoint devices”](#) on page 496.

## 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 492.

**Table 25-3**      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 <a href="#">“Gathering endpoint device IDs”</a> on page 496.
Modify existing endpoint device configurations.	To edit a device definition, select anywhere in the device row, or click the pencil icon.  See <a href="#">“Creating and modifying endpoint device configurations”</a> on page 497.
View configured endpoint devices.	The <b>Endpoint Devices</b> screen lists all configured endpoint devices. The columns display the following information: <ul style="list-style-type: none"> <li>■ Device Name</li> <li>■ Device Description</li> <li>■ Device Definition (Regex)</li> </ul>
Sort endpoint devices.	You can sort the endpoint device list by name, description, or definition.

## 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 496.

### To create and modify endpoint device ID expressions

- 1 Click **Add Device**.  
     Perform this action from the **System > Agent > Endpoint Devices** screen.
- 2 Enter the **Device Name**.
- 3 Enter a **Device Description**.

- 4 Enter the **Device Definition** expression.  
The device definition must conform to the regular expression syntax.  
See [Table 25-4](#) on page 498.  
See [“About writing regular expressions”](#) on page 459.
- 5 Click **Save** to save the device configuration.
- 6 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 498.

**Table 25-4** Example endpoint device expressions

Example device class and expression	
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\\DISKST9160412ASG_____0002SDM1\\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 492.

See [“Manage and add endpoint devices”](#) on page 496.

## 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 338.

**Table 25-5** Configuring the Endpoint Device Class or ID condition

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 <a href="#">“Configuring policy rules”</a> on page 342. See <a href="#">“Configuring policy exceptions”</a> on page 351.
Select one or more devices.	The condition matches when users move data from an endpoint computer to the selected device(s).  Click <b>Create an endpoint device</b> to define one or more devices. See <a href="#">“Creating and modifying endpoint device configurations”</a> on page 497.
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 <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

See [“About endpoint device detection”](#) on page 492.

See [“Manage and add endpoint devices”](#) on page 496.

## 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 338.

**Table 25-6** 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 <a href="#">“Configuring policy rules”</a> on page 342.  See <a href="#">“Configuring policy exceptions”</a> on page 351.
Select the location to monitor.	Select one of the following endpoint locations to monitor: <ul style="list-style-type: none"> <li>■ <b>Off the corporate network</b> Select this option to detect or except events when the endpoint computer is off of the corporate network.</li> <li>■ <b>On the corporate network</b> Select this option to detect or except events when the endpoint computer is on the corporate network. This option is the default selection.</li> </ul> See <a href="#">“About endpoint location detection”</a> on page 493.
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 <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

See [“About endpoint location detection”](#) on page 493.

See [“Endpoint detection best practices”](#) on page 500.

## Endpoint detection best practices

When implementing endpoint detection, consider the following:

- Any detection method that executes on the endpoint matches on the entire message, not individual message components.
- Do not combine an Endpoint Prevent: Notify or Block response rule with two-tier detection methods, including Exact Data Matching, Indexed Document

Matching, or profiled (static) Directory Group Matching. If you do, the system displays a warning for both the policy detection and the response rule.

- 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 [“About detection execution”](#) on page 297.



# Detecting described identities

This chapter includes the following topics:

- [About described identity matching](#)
- [Configuring the Sender/User Matches Pattern condition](#)
- [Configuring the Recipient Matches Pattern condition](#)
- [Described identity matching best practices](#)

## About described identity matching

Described identity detection matches patterns in messages from email senders and recipients, Windows users, IM users, URL domains, and IP addresses.

**Table 26-1** Pattern identity matching examples

Example Pattern	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.

**Table 26-1** Pattern identity matching examples (*continued*)

Example Pattern	Matches	Does Not Match
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. All SMTP email that is addressed to BOB@COMPANY.COM (the pattern is not case-sensitive).	Any email not specifically addressed to bob@company.com, such as: <ul style="list-style-type: none"> <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].  This result assumes that the IP address maps to the desired domain, such as web.company.com.	<b>Note:</b> If the IP address does not match, use one or more domain URLs instead.

See [“Described identity matching best practices”](#) on page 508.

See [“Configuring the Sender/User Matches Pattern condition”](#) on page 504.

See [“Configuring the Recipient Matches Pattern condition”](#) on page 506.

## Configuring the Sender/User Matches Pattern condition

The Sender/User Matches Pattern detection condition matches described user and message sender identities.

You can use this condition in a policy detection rule or exception.

See [“About described identity matching”](#) on page 503.

**Table 26-2**      Configuring the Sender/User Matches Pattern condition

Action	Description
Enter one or more Sender Patterns to match one or more message senders.	<p><b>Email Address Pattern:</b></p> <ul style="list-style-type: none"> <li>■ To match a specific email address, enter the full email address: sales@symantec.com</li> <li>■ To match multiple exact email addresses, enter a comma-separated list: john.smith@company.com, johnsmith@company.com, jsmith@company.com</li> <li>■ To match partial email addresses, enter one or more domain patterns: <ul style="list-style-type: none"> <li>■ Enter one or more top-level domain extensions, for example: .fr, .cu, .in, .jp</li> <li>■ Enter one or more domain names, for example: company.com, symantec.com</li> <li>■ Enter one or more third-level (or lower) domain names: web.company.com, mail.yahoo.com, smtp.gmail.com, dlp.security.symantec.com</li> </ul> </li> </ul>
	<p><b>Windows User Names</b></p> <p>Enter the names of one or more Windows users, for example: john.smith, jsmith</p>
	<p><b>IM Screen Name</b></p> <p>Enter one or more IM screen names that are used in instant messaging systems, for example: john_smith, jsmith</p>
	<p><b>IP Address</b></p> <p>Enter one or more IP addresses that map to the domain you want to match, for example:</p> <ul style="list-style-type: none"> <li>■ Exact IP address match, for example: 192.168.1.1</li> <li>■ Wildcard match – The asterisk (*) character can substitute for one or more fields, for example: 192.168.1.* or 192.*.168.*</li> </ul>

**Table 26-2** Configuring the Sender/User Matches Pattern condition (*continued*)

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 <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

See [“Configuring the Recipient Matches Pattern condition”](#) on page 506.

See [“Described identity matching best practices”](#) on page 508.

## 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 [“About described identity matching”](#) on page 503.

**Table 26-3** Recipient Matches Pattern condition parameters

Action	Description
Enter one or more Recipient Patterns to match one or more message recipients.	<p><b>Email Address/Newsgroup Pattern</b></p> <p>Enter one or more email or newsgroup addresses to match the desired recipients.</p> <p>To match specific email addresses, enter the full address, such as sales@symantec.com. To match email addresses from a specific domain, enter the domain name only, such as symantec.com.</p> <hr/> <p><b>IP Address</b></p> <p>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.</p> <hr/> <p><b>URL Domain</b></p> <p>Enter the URL Domain 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.</p>
Configure match counting.	<p>Select one of the following options to specify the number of email recipients that must match:</p> <ul style="list-style-type: none"> <li>■ <b>All recipients must match (Email Only)</b> does not count a match unless ALL email message recipients match the specified pattern.</li> <li>■ <b>At least _ recipients must match (Email Only)</b> lets you specify the minimum number of email message recipients that must match to be counted.</li> </ul> <p>Select one of the following options to specify how you want to count the matches:</p> <ul style="list-style-type: none"> <li>■ <b>Check for existence</b> Reports a match count of 1 if there are one or more matches.</li> <li>■ <b>Count all matches</b> Reports the sum of all matches.</li> </ul> <p>See <a href="#">“Configuring match counting”</a> on page 346.</p>
Match on the entire message.	<p>This condition matches on the entire message. The <b>Envelope</b> option is selected by default. You cannot select any other message component.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p>

**Table 26-3** Recipient Matches Pattern condition parameters (*continued*)

Action	Description
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 “ <a href="#">Configuring compound match conditions</a> ” on page 354.

See “[Configuring the Sender/User Matches Pattern condition](#)” on page 504.

See “[Described identity matching best practices](#)” on page 508.

## Described identity matching best practices

Keep in mind the following considerations when you implement the Sender/User or Recipient Matches Pattern conditions in policy detection rules or exceptions:

- 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 “[About detection execution](#)” on page 297.
- 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 “[About described identity matching](#)” on page 503.
- 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`.
- 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 .

See [“Configuring the Sender/User Matches Pattern condition”](#) on page 504.

See [“Configuring the Recipient Matches Pattern condition”](#) on page 506.



# Detecting synchronized identities

This chapter includes the following topics:

- [About implementing synchronized Directory Group Matching](#)
- [About connecting to directory group servers](#)
- [Creating and managing directory server connections](#)
- [Scheduling directory server indexing](#)
- [Creating or modifying a User Group](#)
- [Configuring the Sender/User matches User Group based on a Directory Server condition](#)
- [Configuring the Recipient Matches User Group based on a Directory Server condition](#)
- [Synchronized DGM best practices](#)

## About implementing synchronized Directory Group Matching

Symantec Data Loss Prevention provides Directory Group Matching (DGM) to detect the exact identities of users, senders, and recipients.

See [“About Directory Group Matching”](#) on page 287.

You can connect the Enforce Server or a Discover Server to a group directory server to detect users based on their group affiliation. For example, you want to

apply policies to staff in the engineering department of your company but not to staff in the human resources department.

You select the group from the users, groups, and business units that are defined in your company's directory server. After the user group is constructed, you can associate it with the User/Sender and Recipient conditions, or with Discover targets. After you apply the policy or target to the group, it only applies to users who are in the group. If the identity being detected is users, the user must be actively logged on to their agent-enabled system. Or, an alternate example is that you want to create a policy that applies to your entire company except the CEO. You can create a user group that contains only the CEO as a member and use that group as an exception to the policy. You can create any number of groups based on any specifications you want.

The connection to each directory server group that you want to use is called a Group Directory. The Group Directory connection specifies the directory server you want to use as source information for defining exact identity user groups. The identity group editing page is where you use the source information to create identity groups.

**Table 27-1** Detecting identity from a synchronized directory group server

Step	Task	Description
1	Create the connection to the directory server.	Establish the connection from the Enforce Server or a Discover Server to the directory server with configured users and groups.  See <a href="#">“Creating and managing directory server connections”</a> on page 513.
2	Create the User Group(s).	Create one or more User Groups on the Enforce Server and populate them with identities from Microsoft Active Directory.  See <a href="#">“Creating or modifying a User Group”</a> on page 517.
3	Create a policy.	Configure a new policy or edit an existing one.  See <a href="#">“About User Groups”</a> on page 317. See <a href="#">“Configuring policies”</a> on page 338.

**Table 27-1** Detecting identity from a synchronized directory group server  
*(continued)*

Step	Task	Description
4	Configure one or more User Group rules or exceptions.	<p>Add the user group rule or exception to the policy.</p> <p>After the policy and the group are linked, the policy applies only to that group.</p> <p>See <a href="#">“Configuring the Sender/User matches User Group based on a Directory Server condition”</a> on page 519.</p> <p>See <a href="#">“Configuring the Recipient Matches User Group based on a Directory Server condition”</a> on page 520.</p>

## About connecting to directory group servers

Symantec Data Loss Prevention supports directory server connections to Microsoft Active Directory (AD). The group directory connection specifies how the Enforce Server or Discover Server connects to the Active Directory server for populating and synchronizing User Groups for identity-based detection.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

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 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 [“Creating or modifying a User Group”](#) on page 517.

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 168.

## Creating and managing directory server connections

The **System > Settings > Group Directories** screen is the home page for creating and managing directory group server connections. You must establish the connection to the directory server before you create User Groups.

See [“About connecting to directory group servers”](#) on page 513.

**Table 27-2** Manage group directory server connections

Action	Description
Create new connection, or modify an existing one.	Click the <b>Create New Connection</b> to create a new connection. Select the directory connection in the <b>Group Directories</b> screen to modify it. See <a href="#">Table 27-3</a> on page 514.
Schedule and monitor directory indexing.	Each group directory connection is set to automatically index the configured User Groups hosted in the directory server <b>once</b> 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. See <a href="#">“Scheduling directory server indexing”</a> on page 516. View the indexing status in the <b>Index and Replication Status</b> tab for the directory connection.
Manage existing connections.	The <b>Group Directories</b> screen lists the current group directory connections. You can view and sort existing connections by: <ul style="list-style-type: none"> <li>■ <b>Connection Name:</b> The user-defined name for the connection.</li> <li>■ <b>Hostname:</b> The hostname of the computer where the directory server is installed.</li> <li>■ <b>Base DN:</b> The base distinguished name of the directory server.</li> <li>■ <b>Port:</b> The port that enables directory server connections.</li> <li>■ <b>Encryption Method:</b> None or Secure.</li> </ul> See <a href="#">“Importing SSL certificates to Enforce or Discover servers”</a> on page 168.
Delete an existing connection.	Click the delete icon.

**Table 27-3** Configuring a group directory server connection to Active Directory

General Settings	Description
Name the connection.	Enter the <b>Name</b> that you want to call this connection. Use a descriptive name that easily identifies the connection.

**Table 27-3**      Configuring a group directory server connection to Active Directory  
*(continued)*

General Settings	Description
Provide the hostname of the directory server.	The <b>Hostname</b> of the directory server. For example, <b>example.symantec.com</b> .
Specify the connection port.	The <b>Port</b> is the network port over which the directory server and the Enforce Server communicate. Typically, you should use port number 389 or 636 for secure connections.
Enter the Base DN.	<p>The <b>Base DN</b> is the base distinguished name of the directory server. Typically, this name is the domain name of the AD server. Generally, use codes to distinguish each part of the domain name. For example, the code DC=. If you wanted to connect to the server <b>example.symantec.com</b>, you would use the following terminology to define the base DN:</p> <p>DC=example, DC=symantec, DC=com</p> <p><b>Note:</b> If you are not familiar with distinguished names or your AD server, contact your AD server administrator to obtain your AD distinguished name.</p>
Select the encryption method.	<p>Select the <b>Encryption Method</b> option if you want the communication between the AD server and the Enforce Server to be encrypted using SSL. By default, this field is set to None.</p> <p><b>Note:</b> If you chose to use a secure connection, SSL, you may need to import the AD server security certificate into the Enforce Server keystore. See <a href="#">“Importing SSL certificates to Enforce or Discover servers”</a> on page 168.</p>
Specify the authentication method.	<p>Select if you want to allow anonymous <b>Authentication</b> connections to the AD server or if you want to require user names and passwords for every connection.</p> <p>Most AD servers do not allow anonymous connections.</p>
Enter the username to connect to the directory server.	<p>The user name to authenticate the AD connection.</p> <p>You can enter the user name as one of the following:</p> <ul style="list-style-type: none"> <li>■ Windows logon (Enterprise\firstname_lastname)</li> <li>■ Username and domain (username@domain.com)</li> </ul> <p>Full distinguished name of the user within the AD server (cn=user name, cn=Users, dc=domain, dc=com)</p>
Password	The password to authenticate the AD connection.

**Table 27-3** Configuring a group directory server connection to Active Directory  
*(continued)*

General Settings	Description
Test Connection	Click <b>Test Connection</b> . The Enforce Server tests the connection. If there is anything wrong with the connection, the system displays an error message describing the problem.
Save the connection.	Click <b>Save</b> to save the connection configuration.
Schedule indexing.	See “ <a href="#">Scheduling directory server indexing</a> ” on page 516.

See “[About User Groups](#)” on page 317.

## Scheduling directory server indexing

After you create, test, and save the directory server connection, the system automatically indexes all 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 > Group Directories** screen. Or, create a new connection.

See “[Creating and managing directory server connections](#)” on page 513.

- 2 Adjust the Index Settings to the desired schedule.

See [Table 27-4](#) on page 516.

**Table 27-4** Schedule group directory server indexing and view status

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.

**Table 27-4** Schedule group directory server indexing and view status (*continued*)

Index Settings	Description
Index the directory server daily.	Select the <b>Daily</b> option to schedule the index 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 <b>day of the week</b> to index.  Specify the <b>time</b> to index.  Optionally, specify the <b>Until</b> duration for this schedule.
Index the directory server monthly.	Specify the <b>day of the month</b> to index the directory and the <b>time</b> .  Optionally, specify the <b>Until</b> 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.  <ul style="list-style-type: none"> <li>■ <b>Indexing Status</b> Displays the next scheduled index, date and time.</li> <li>■ <b>Detection Server Name</b> Displays the detection server where the User Group profile is deployed.</li> <li>■ <b>Replication Status</b> ■ Displays the data and time of the most recent synchronization with the directory group server.</li> </ul>

## Creating or modifying a User Group

The **Manage > Policies > User Groups** screen displays configured User Groups and is the starting point for creating a new User Group.

See “[About User Groups](#)” on page 317.

### To create or modify a User Group

- 1 Establish a connection to the Active Directory server you want to synchronize with.  
  
See “[Creating and managing directory server connections](#)” on page 513.
- 2 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 27-5](#) on page 518.
- 4 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**.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

**Table 27-5** Configure a User Group

Action	Description
Enter the group name.	The <b>Group Name</b> is the name that you want to use to identify this group. 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 use the group.	Initially, when you create a new User Group, the <b>Used in Policy</b> field displays <b>None</b> . 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.	Select the <b>Refresh the group directory index on Save</b> option to synchronize the User Group profile with the latest index replication. The system synchronizes the profile with the latest index when you <b>Save</b> the profile. See <a href="#">“Scheduling directory server indexing”</a> on page 516.
Select the directory server.	Select the directory server you want to use from the <b>Directory Server</b> list. You must establish a connection to the directory server before you create the User Group profile. See <a href="#">“Creating and managing directory server connections”</a> on page 513.

## Configuring the Sender/User matches User Group based on a Directory Server condition

Table 27-5 Configure a User Group (*continued*)

Action	Description
Browse the directory for user groups.	<p>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.</p> <p>The browse results display the name of each node. These names give you the specific user identity.</p> <p>The results are limited to 20 entries by default. Click <b>See More</b> to view up to 1000 results.</p>
Add a user group to the profile.	<p>To add a group or user to the User Group profile, select it from the tree and click <b>Add</b>.</p> <p>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).</p>
Search the directory for specific users.	<p>The <b>Search Directory</b> field lets you search the directory for specific users. You can <b>Search</b> the directory using the following search criteria:</p> <ul style="list-style-type: none"> <li>■ Name of individual node</li> <li>■ Email address</li> </ul> <p>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.</p> <p>The <b>Clear</b> option returns you to the Browse Directory function. Enter a new search string into the Search field to activate the Search Directory function.</p>
Save the user group.	Click <b>Save</b> to save the User Group profile you have configured.

## Configuring the Sender/User matches User Group based on a Directory Server condition

The Sender/User matches User Group based on a Directory Server condition matches policy violations based on message senders and endpoint computer 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 338.

**Table 27-6** Sender/User matches User Group condition parameters

Parameter	Description
Select User Groups to include in this policy	Select one or more User Groups that you want this policy to detect. If you have not created a User Group, click <b>Create a new User Group</b> . See <a href="#">“Creating or modifying a User Group”</a> on page 517.
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 <a href="#">“About message components that can be matched”</a> on page 293.
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 <a href="#">“Configuring compound match conditions”</a> on page 354.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

See [“Synchronized DGM best practices”](#) on page 521.

## Configuring the Recipient Matches User Group based on a Directory Server condition

The Recipient matches User Group based on a Directory Server Group condition matches policy violations based on specific message recipients synchronized from a directory group server.

You can implement this condition in a policy group (identity) rule or exception.

See [“Configuring policies”](#) on page 338.

**Table 27-7** Recipient matches User Group based on a Directory Server Group condition

Parameter	Description
Select User Groups to include in this policy	Select the User Group(s) that you want this policy to match on. If you have not created a User Group, click <b>Create a new Endpoint User Group</b> option. See <a href="#">“Creating or modifying a User Group”</a> on page 517.

**Table 27-7** Recipient matches User Group based on a Directory Server Group condition (*continued*)

Parameter	Description
Match On	<p>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.</p> <p>See <a href="#">“About message components that can be matched”</a> on page 293.</p>
Also Match	<p>Select this option to create a compound condition. All conditions in a rule or exception must match to trigger an incident.</p> <p>You can <b>Add</b> any available condition from the list.</p> <p>See <a href="#">“Configuring compound match conditions”</a> on page 354.</p>

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

See [“Synchronized DGM best practices”](#) on page 521.

## Synchronized DGM best practices

When implementing user group directory server policies, consider the following:

- If you combine a user group condition with a detection condition in a single policy, the rules are ANDed together. The result is that both conditions must match for the policy to trigger an incident.  
 See [“About message components that can be matched”](#) on page 293.
- If you apply either the Sender/User or Recipient conditions to a non-endpoint detection server, the condition is not ignored. Instead, the group-based condition fails and causes the policy to ignore possible violations because all conditions are not met. If you want to apply a policy to non-endpoint detection messages, do not include a group-based condition in that policy.
- Identity-based detection involving users applies to the users in a configured group of DLP Agent-based endpoint computers. With endpoint 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 computer varies depending on how the users are grouped. Contrast this style of endpoint detection with the endpoint destination or location methods, which are specific to the endpoint computer and are not user-based.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.



# Detecting profiled identities

This chapter includes the following topics:

- [About implementing profiled Directory Group Matching](#)
- [Creating the Exact Data Profile for static DGM](#)
- [Configuring the Sender/User Matches Directory From Exact Data Profile condition](#)
- [Configuring the Recipient Matches Directory From Exact Data Profile condition](#)
- [Profiled DGM best practices](#)

## About implementing profiled Directory Group Matching

Symantec Data Loss Prevention lets you detect the exact identities of data users, message senders, and recipients based on a profiled directory server or database.

Symantec Data Loss Prevention provides two static Directory Group Matching methods. Both methods require the use of an Exact Data Profile with specific data fields.

**Table 28-1** Profiled Directory Group Matching detection rules

Group rule	Description
Sender/User Matches Directory From Exact Data Profile	Group-related attributes may include an IP address, email, Windows user name, business unit, department, manager, title, employment status. Other attributes may be whether that employee has provided consent to be monitored, or whether the employee has access to sensitive information.

**Table 28-1** Profiled Directory Group Matching detection rules (*continued*)

Group rule	Description
For the Recipient Matches Directory From Exact Data Profile	You can index a list of recipients email addresses and author policies based on this indexed data. For example, you can write a detection rule that requires the message sender to be from the customer service department to violate the policy. Or, you could write a detection exception that is not violated if the recipient of an email is on an approved list.

See [“About Directory Group Matching”](#) on page 287.

## Creating the Exact Data Profile for static DGM

Profiled DGM requires the use of an exact data source with specific data fields.

### To create the exact data source file for DGM

- 1 Create a data source file for the directory server or database you want to profile.  
See [“Creating the exact data source file”](#) on page 374.
- 2 To implement profiled DGM, the system requires one or more specific data element types to detect the message user, sender, or recipient.

The exact data source file must contain one or more of the following fields:

- Email address
- IP address
- Windows user name
- AOL IM name
- Yahoo! IM name
- MSN IM name

- 3 Prepare the data source file for indexing and upload the data source file available to the Enforce Server.  
 See [“Preparing the exact data source file for indexing”](#) on page 376.  
 See [“Uploading exact data source files to the Enforce Server”](#) on page 378.
- 4 Create the Exact Data Profile, map the data fields, and index the data source.  
 See [“Creating and modifying Exact Data Profiles”](#) on page 379.  
 See [“Mapping Exact Data Profile fields”](#) on page 384.  
 See [“Scheduling Exact Data Profile indexing”](#) on page 386.

## Configuring the Sender/User Matches Directory From Exact Data Profile condition

The Sender/User Matches Directory From detection rule lets you create detection rules based on sender identity or (for endpoint incidents) user identity.

The Sender/User Matches Directory From detection rule relies on EDM detection technology and requires an Exact Data Profile.

See [“About implementing Exact Data Matching”](#) on page 368.

After you select the Data Profile, when you configure the rule, the directory you selected and the sender identifier(s) appear at the top of the page.

**Table 28-2** Configuring the Sender/User Matches Directory From Exact Data Profile condition

Parameter	Description
Where	Select this option to have Symantec Data Loss Prevention 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 Department field, select Where, select <b>Department</b> from the drop-down list, and type <b>Marketing,Sales</b> in the text box. For a detection rule, this example causes Symantec Data Loss Prevention to capture an incident only if the sender or user works in Marketing or Sales (as long as the input content meets all other detection criteria). For an exception, this example prevents Symantec Data Loss Prevention from capturing an incident if the sender or user works in Marketing or Sales.

**Table 28-2** Configuring the Sender/User Matches Directory From Exact Data Profile condition (*continued*)

Parameter	Description
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 Matches Directory From Exact Data Profile condition

The Recipient Matches Directory From detection rule lets you create detection methods based on the identity of the recipient. This method requires an Exact Data Profile.

See [“About implementing Exact Data Matching”](#) on page 368.

After you select the Data Profile, when you configure the rule, the directory you selected and the recipient identifier(s) appear at the top of the page.

**Table 28-3** Configuring the Recipient Matches Directory From Exact Data Profile condition

Parameter	Description
Where	Select this option to have Symantec Data Loss Prevention 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 Department field, select Where, select <b>Department</b> from the drop-down list, and enter <b>Marketing, Sales</b> in the text box. For a detection rule, this example causes Symantec Data Loss Prevention 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 Symantec Data Loss Prevention 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.

## Profiled DGM best practices

Keep in mind the following considerations when implementing profiled Directory Group Matching:

- You must include the appropriate fields in the Exact Data Profile to implement profiled DGM.  
See [“Creating the Exact Data Profile for static DGM”](#) on page 524.
- You cannot use the Sender/User Matches Directory or the Recipient Matches Directory conditions in policy exceptions. To except message users, senders, and recipients from detection, use the identity pattern matching conditions.  
See [“About described identity matching”](#) on page 503.
- To except data owners from detection, you must include the users email address or email domain in the Data Profile.  
See [“About data owner exception”](#) on page 370.
- You cannot combine a Sender/User Matches Directory From group rule with an Endpoint: Block or Endpoint: Notify response rule in a policy. If you do, the system reports that the policy is misconfigured.
- You cannot combine a Recipient Matches Directory From group rule with an Endpoint: Block or Endpoint: Notify response rule in a policy. If you do, the system reports that the policy is misconfigured.



# Detecting international content

This chapter includes the following topics:

- [About implementing non-English language detection](#)
- [International policy templates](#)
- [Using find keywords for international system data identifiers](#)
- [Detecting non-English document content](#)

## About implementing non-English language detection

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 55.

See [“Working with international characters”](#) on page 58.

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 56.

See [“International policy templates”](#) on page 530.

See [“Using find keywords for international system data identifiers”](#) on page 531.

See [“Detecting non-English document content”](#) on page 533.

# International policy templates

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 321.

**Table 29-1** International policy templates

Policy template	Description
Canadian Social Insurance Numbers	This policy detects patterns indicating Canadian social insurance numbers.  See <a href="#">“Canadian Social Insurance Numbers policy template”</a> on page 605.
Caldicott Report	This policy protects UK patient information.  See <a href="#">“Caldicott Report policy template”</a> on page 603.
UK Data Protection Act 1998	This policy protects personal identifiable information.  See <a href="#">“Data Protection Act 1998 (UK) policy template”</a> on page 611.
EU Data Protection Directives	This policy detects personal data specific to the EU directives.  See <a href="#">“Data Protection Directives (EU) policy template”</a> on page 612.
UK Human Rights Act 1998	This policy enforces Article 8 of the act for UK citizens.  See <a href="#">“Human Rights Act 1998 policy template”</a> on page 631.
PIPEDA (Canada)	This policy detects Canadian citizen customer data.  See <a href="#">“PIPEDA policy template”</a> on page 649.
SWIFT Codes (International banking)	This policy detects codes that banks use to transfer money across international borders.  See <a href="#">“SWIFT Codes policy template”</a> on page 666.
UK Drivers License Numbers	This policy detects UK Drivers License Numbers.  See <a href="#">“UK Drivers License Numbers policy template”</a> on page 667.
UK Electoral Roll Numbers	This policy detects UK Electoral Roll Numbers.  See <a href="#">“UK Electoral Roll Numbers policy template”</a> on page 667.

**Table 29-1** International policy templates (*continued*)

Policy template	Description
UK National Insurance Numbers	This policy detects UK National Insurance Numbers. See <a href="#">“UK National Insurance Numbers policy template”</a> on page 668.
UK National Health Service Number	This policy detects personal identification numbers issued by the NHS. See <a href="#">“UK National Health Service (NHS) Number policy template”</a> on page 668.
UK Passport Numbers	This policy detects valid UK passports. See <a href="#">“UK Passport Numbers policy template”</a> on page 669.
UK Tax ID Numbers	This policy detects UK Tax ID Numbers. See <a href="#">“UK Tax ID Numbers policy template”</a> on page 669.

## Using find keywords for international system data identifiers

Data identifiers offer broad support for detecting international content.

See [“About data identifiers”](#) on page 416.

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 system data identifier breadth”](#) on page 436.

The following table provides keywords for several international data identifiers.

**To use keywords for international data identifiers**

- 1 Create a policy using one of the system-provided international data identifiers that is listed in the table.  
 See [Table 29-2](#) on page 532.
- 2 Select the **Find Keywords** optional validator.  
 See [“Configuring the Content Matches Data Identifier condition”](#) on page 434.
- 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 440.

**Table 29-2** 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 fiscale, 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

**Table 29-2** International Data Identifiers and Keyword Lists (*continued*)

Data Identifier	Language	Keywords	English Translation
People's Republic of China ID	Chinese (Simplified)	身份证,居民信息,居民身份证信息	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
Swiss AHV Number	French	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité sociale, Numéro AVH	AVS number, insurance number, national identifier, national insurance number, social security number, AVH number
	German	AHV-Nummer, Matrikelnummer, Personenidentifikationsnummer	AHV number, Swiss Registration number, PIN
	Italian	AVS, AVH	AVS, AVH
Taiwan ROC ID	Chinese (Traditional)	中華民國國民身分證	ROC ID

## Detecting non-English document content

The detection engine uses Unicode internally and supports content, context, and identity matching for all detection technologies in any supported language.

See [“About implementing non-English language detection”](#) on page 529.

Indexed Document Matching (IDM) supports document content detection in non-English languages, including Asian languages that use double-byte character sets.

See [“About implementing Indexed Document Matching”](#) on page 393.

When you index documents for an IDM profile, the system ignores commonly used words known as stopwords. Symantec Data Loss Prevention provides several stopword files in the directory `\Vontu\Protect\config\stopwords`. By default the system is set to ignore common English language stopwords in the

`stopwords_en.txt` file. When you configure a detection server, you can change the default stopword file to another supported language, or you can add multiple stopword files for mixed-language use cases. To do this, adjust the value for the **Lexer.StopwordLanguages** setting.

See [“Advanced server settings”](#) on page 174.

# System data identifiers

This chapter includes the following topics:

- [ABA Routing Number system data identifier](#)
- [Australian Medicare Number system data identifier](#)
- [Australian Tax File Number system data identifier](#)
- [Burgerservicenummer system data identifier](#)
- [Canadian Social Insurance Number system data identifier](#)
- [Codice Fiscale system data identifier](#)
- [Credit Card Magnetic Stripe Data system data identifier](#)
- [Credit Card Number system data identifier](#)
- [CUSIP Number system data identifier](#)
- [Drivers License Number – CA State system data identifier](#)
- [Drivers License Number - FL, MI, MN States system data identifier](#)
- [Drivers License Number - IL State system data identifier](#)
- [Drivers License Number - NJ State system data identifier](#)
- [Drivers License Number - NY State system data identifier](#)
- [French INSEE Code system data identifier](#)
- [Hong Kong ID system data identifier](#)
- [IBAN Central system data identifier](#)
- [IBAN East system data identifier](#)

- [IBAN West system data identifier](#)
- [IP Address system data identifier](#)
- [National Drug Code \(NDC\) system data identifier](#)
- [People's Republic of China ID system data identifier](#)
- [Singapore NRIC system data identifier](#)
- [South Korea Resident Registration Number system data identifier](#)
- [Spanish DNI ID system data identifier](#)
- [SWIFT Code system data identifier](#)
- [Swiss AHV Number system data identifier](#)
- [Taiwan ROC ID system data identifier](#)
- [UK Drivers License Number system data identifier](#)
- [UK Electoral Roll Number system data identifier](#)
- [UK National Health Service \(NHS\) Number system data identifier](#)
- [UK National Insurance Number system data identifier](#)
- [UK Passport Number system data identifier](#)
- [UK Tax ID Number system data identifier](#)
- [US Individual Tax Identification Number \(ITIN\) system data identifier](#)
- [US Social Security Number \(SSN\) system data identifier](#)

## ABA Routing Number system 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 system 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 537.

- 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 537.
- 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 538.

## ABA Routing Number wide breadth

The wide breadth edition of the ABA Routing Number system data identifier detects 9-digit numbers. It validates the number using the final check digit.

**Table 30-1** ABA Routing Number wide breadth patterns

Pattern
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

**Table 30-2** 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 system 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 30-3** ABA Routing Number medium breadth patterns

Pattern
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

**Table 30-4** 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 system 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 30-5** ABA Routing Number narrow breadth patterns

Pattern
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

**Table 30-6** 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.

**Table 30-6** ABA Routing Number narrow breadth validators (*continued*)

Mandatory validator	Description
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, bankrouting#, bankroutingnumber
Number delimiter	Validates a match by checking the surrounding numbers.

## Australian Medicare Number system 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 system 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.

**Table 30-7** Australian Medicare Number wide breadth patterns

Pattern
<code>\d{4} \d{5} \d \d</code>
<code>\d{4}-\d{5}-\d-\d</code>

## Australian Tax File Number system 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 system data identifier detects an 8- or 9-digit number and ensures that the detected number passes checksum validation.

**Table 30-8** Australian Tax File Number wide breadth patterns

Pattern
<code>\d{8}</code>
<code>\d{9}</code>

**Table 30-9** Australian Tax File Number wide breadth validator

Mandatory validator	Description
Australian Tax File validation check	Computes the checksum and validates the pattern against it.

## Burgerservicenummer system 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 system data identifier detects an 8- or 9-digit number that passes checksum validation.

**Table 30-10** Burgerservicenummer wide breadth pattern

Pattern
<code>\d{9}</code>

**Table 30-11** Burgerservicenummer wide breadth validator

Mandatory validator	Description
Burgerservicenummer Check	Burgerservicenummer Check.

# Canadian Social Insurance Number system 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 system data identifier provides three breadths of detection:

- **Wide**  
See “[Canadian Social Insurance Number wide breadth](#)” on page 541.
- **Medium**  
See “[Canadian Social Insurance Number medium breadth](#)” on page 542.
- **Narrow**  
See “[Canadian Social Insurance Number narrow breadth](#)” on page 542.

## Canadian Social Insurance Number wide breadth

The wide breadth Canadian Social Insurance Number system DI detects 9-digit numbers with the format DDD-DDD-DDD separated by dashes, spaces, periods, slashes, or without separators. Performs Luhn check validation.

**Table 30-12** 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 30-13** Canadian Social Insurance Number wide breadth validator

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 system DI detects 9-digit numbers with the format DDD-DDD-DDD separated by dashes, spaces, or periods. It performs Luhn check validation and eliminates non-assigned numbers and common test numbers.

**Table 30-14** Canadian Social Insurance Number medium breadth patterns

Pattern
\d{3} \d{3} \d{3}
\d{3}.\d{3}.\d{3}
\d{3}-\d{3}-\d{3}

**Table 30-15** Canadian Social Insurance Number medium 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: 8, 123456789

## Canadian Social Insurance Number narrow breadth

The narrow breadth Canadian Social Insurance Number system DI detects 9-digit numbers with the format DDD-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 30-16** Canadian Social Insurance Number narrow breadth patterns

Pattern
\d{3} \d{3} \d{3}

**Table 30-16** Canadian Social Insurance Number narrow breadth patterns  
*(continued)*

Pattern
\d{3}-\d{3}-\d{3}

**Table 30-17** 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 system 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 system data identifier detects a 16 character identifier. The final character must match a checksum algorithm.

**Table 30-18** Codice Fiscale wide breadth patterns

Pattern
[A-Z]{6}[0-9LMNPQRSTU]{2}[ABCDEHLMPRST][0-9LMNPQRSTU]{2}[A-Z] [0-9LMNPQRSTU]{3}[A-Z]
[A-Z]{3}[A-Z]{3}[0-9LMNPQRSTU]{2}[ABCDEHLMPRST][0-9LMNPQRSTU]{2} [A-Z][0-9LMNPQRSTU]{3}[A-Z]

**Table 30-19** 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 system 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 system 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 system 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, discretionary data, and the end sentinel. It also includes standard field separators. It validates the data using a Luhn check validator.

**Table 30-20** Credit Card Magnetic Stripe Data medium breadth 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}-\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}-\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} \d{4}^[A-Z]{1}	
%B6011\d{12}^[A-Z]{1}	

**Table 30-21** Credit Card Magnetic Stripe Data medium breadth validator

Validator	Description
Luhn Check	Computes the Luhn checksum which every instance must pass.

## Credit Card Number system 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 system data identifier offers three breadths of detection:

- Wide breadth  
See “[Credit Card Number wide breadth](#)” on page 546.
- Medium breadth  
See “[Credit Card Number medium breadth](#)” on page 547.
- Narrow breadth  
See “[Credit Card Number narrow breadth](#)” on page 549.

### Credit Card Number wide breadth

The wide breadth Credit Card Number system 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 30-22** Credit Card Number wide breadth patterns

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}-\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 30-23** Canadian Social Insurance 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 system 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 30-24** 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}.\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}.\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}	

**Table 30-25** Credit Card Number medium 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.

**Table 30-25** Credit Card Number medium breadth validators (*continued*)

Mandatory validator	Description
Exclude data match inputs	0111111111111111, 1234567812345670, 180025848680889, 180026939516875, 201400000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 300000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 340000000000009, 341019464477148, 3411111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 3700000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 40070000000027, 4012888888881880, 4024007116284, 4111111111111110, 4111111111111111, 42222222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 5431111111111111, 5455780586062610, 5472715456453270, 5500000000000004, 5539878514522540, 5547392938355060, 5555555555554440, 5555555555554444, 5556722757422205, 6011000000000000, 6011000000000004, 6011000000000012, 6011000990139420, 6011111111111110, 6011111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071
Number Delimiter	Validates a match by checking the surrounding number.

## Credit Card Number narrow breadth

The narrow breadth edition of the Credit Card Number system 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 30-26** 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}-\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 30-27** 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, 201400000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 300000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 340000000000009, 341019464477148, 3411111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 4007000000027, 401288888881880, 4024007116284, 4111111111111110, 4111111111111111, 42222222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 5431111111111111, 5455780586062610, 5472715456453270, 5500000000000004, 5539878514522540, 5547392938355060, 5555555555554440, 5555555555554444, 5556722757422205, 6011000000000000, 6011000000000004, 6011000000000012, 6011000990139420, 6011111111111110, 6011111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071
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.

**Table 30-27** Credit Card Number narrow breadth validators (*continued*)

Mandatory validator	Description
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, enrout, japanese card bureau, jcb, mastercard, mc, visa

## CUSIP Number system 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 system 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 552.
- The medium edition validates the final check digit and requires the presence of a keyword.  
See [“CUSIP Number medium breadth”](#) on page 553.
- The narrow edition validates the final check digit and requires the presence of a keyword.  
See [“CUSIP Number narrow breadth”](#) on page 553.

## CUSIP Number wide breadth

The wide breadth edition of the CUSIP Number system 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 30-28** CUSIP Number wide breadth pattern

Pattern
<code>\d{4}\w{4}\d</code>

**Table 30-29** 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 wide breadth edition of the CUSIP Number system 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 30-30** CUSIP Number medium breadth pattern

Pattern
<code>\d{4}\w{4}\d</code>

**Table 30-31** CUSIP Number medium breadth validator

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 wide breadth edition of the CUSIP Number system 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 30-32** CUSIP Number narrow breadth pattern

Pattern
<code>\d{4}\w{4}\d</code>

**Table 30-33** 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.
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 system 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 system 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 554.
- The medium breadth edition validates a detected number against keywords.  
 See [“Drivers License Number – CA State medium breadth”](#) on page 555.

### Drivers License Number – CA State wide breadth

The wide breadth edition of the CA Driver License Number system 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 30-34** Drivers License Number wide breadth pattern

Pattern
\d{7}

---

## Drivers License Number – CA State medium breadth

The medium breadth edition of this system 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 30-35** Drivers License Number – CA State medium breadth pattern

Pattern
\d{7}

---

**Table 30-36** 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 - FL, MI, MN States system data identifier

These numbers 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 system 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 556.
- The medium breadth narrows the scope by requiring the presence keywords.  
See [“Drivers License Number- FL, MI, MN States medium breadth”](#) on page 556.

## Drivers License Number- FL, MI, MN States wide breadth

The wide breadth edition of this system 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 30-37** Drivers License Number- FL, MI, MN States wide breadth patterns

Patterns
<code>\\l \\d{3} \\d{3} \\d{3} \\d{3}</code>
<code>\\d{12}</code>
<code>\\d{3}-\\d{3}-\\d{2}-\\d{3}-\\d</code>
<code>\\l-\\d{3}-\\d{3}-\\d{3}-\\d{3}</code>

---

## Drivers License Number- FL, MI, MN States medium breadth

The medium breadth edition of this data identifier implements patterns 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 30-38** Drivers License Number- FL, MI, MN States medium breadth patterns

Pattern
<code>\\l \\d{3} \\d{3} \\d{3} \\d{3}</code>
<code>\\d{12}</code>
<code>\\d{3}-\\d{3}-\\d{2}-\\d{3}-\\d</code>
<code>\\l-\\d{3}-\\d{3}-\\d{3}-\\d{3}</code>

**Table 30-39**

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 - IL State system 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 system 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 558.
- The medium breadth narrows the scope by requiring the presence of keywords. See [“Drivers License Number- IL State medium breadth”](#) on page 558.

## Drivers License Number- IL State wide breadth

The wide breadth edition of the Drivers License Number- IL State system 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 30-40** Drivers License Number- IL State wide breadth patterns

Pattern
\\I\\d{3}-\\d{4}-\\d{4}
\\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 30-41** Drivers License Number- IL State medium breadth patterns

Pattern
\\I\\d{3}-\\d{4}-\\d{4}
\\d{11}

**Table 30-42** Drivers License Number- IL State medium breadth validators

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#

**Table 30-42** Drivers License Number- IL State medium breadth validators  
*(continued)*

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	il, illinois

## Drivers License Number - NJ State system 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 system 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 559.
- The medium breadth narrows the scope by requiring the presence of keywords. See [“Drivers License Number- NJ State medium breadth”](#) on page 560.

### Drivers License Number- NJ State wide breadth

The wide breadth edition of the Drivers License Number- NJ State system 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 30-43** Drivers License Number- NJ State wide breadth patterns

Patterns
\\I\\d{4} \\d{5} \\d{5}
\\d{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.

**Table 30-44** Drivers License Number- NJ State medium breadth patterns

Pattern
\\l\\d{3}-\\d{4}-\\d{4}
\\d{11}

**Table 30-45** 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.
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 - NY State system 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 system 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 559.

- The medium breadth narrows the scope by requiring the presence of keywords. See “[Drivers License Number- NJ State medium breadth](#)” on page 560.

## Drivers License Number- NY State wide breadth

The wide breadth edition of the Drivers License Number- NY State system data identifier detects a 9-digit string.

---

**Note:** The wide breadth option does not include any validators.

---

**Table 30-46** Drivers License Number- NY 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 30-47** Drivers License Number- NY State wide breadth patterns

Pattern
\\l\\d{3}-\\d{4}-\\d{4}
\\l\\d{11}

**Table 30-48**

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#

**Table 30-48** (continued)

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	new york, ny, newyork

## French INSEE Code system 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 system data identifier detects the presence of INSEE numbers.

The wide breadth edition of the French INSEE Code system 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 30-49** French INSEE Code wide breadth patterns

Pattern
\d{13} \d{2}
d{15}

**Table 30-50** 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 system 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 system data identifier detects the presence of Hong Kong IDs.

The wide breadth edition of the Hong Kong ID system data identifier detects 8 characters in the form LDDDDDD(D) or LDDDDDD(A). The last character in the detected string is used to validate a checksum.

**Table 30-51** Hong Kong ID wide breadth patterns

Patterns
<code>\w\d{6}(\d)</code>
<code>\w\d{6}(A)</code>
<code>U\w\d{6}(\d)</code>
<code>U\w\d{6}(A)</code>

**Table 30-52** Hong Kong ID wide breadth validator

Mandatory validator	Description
Hong Kong ID	Computes the checksum and validates the pattern against it.

## IBAN Central system data identifier

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN Central system 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 system data identifier detects a country-specific IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

**Table 30-53** IBAN Central wide breadth patterns

Pattern	Description
<code>AD\d{2}\d{4}\d{4}\w{4}\w{4}</code>	Andorra patterns
<code>AD\d{2} \d{4} \d{4} \w{4} \w{4}</code>	
<code>AD\d{2}-\d{4}-\d{4}-\w{4}-\w{4}</code>	

**Table 30-53** IBAN Central wide breadth patterns (*continued*)

Pattern	Description
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}-\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}-\d{4}	
CH\d{2}\d{4}\d{w{3}}\w{4}\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{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{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	
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}-\w{4}	
MC\d{2}\d{4}\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\d{2}	
MC\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w\d{2}	

**Table 30-53** IBAN Central wide breadth patterns (*continued*)

Pattern	Description
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\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 30-54** IBAN Central wide breadth validator

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

## IBAN East system data identifier

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN East system 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 system data identifier detects a country-specific IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

**Table 30-55** 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}-\d{4}	

**Table 30-55** IBAN East wide breadth patterns (continued)

Pattern	Description
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}-\w{4}	
CZ\d{2}\d{4}\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}-\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}-\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{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{4}-\d	
HU\d{2}\d{4}\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}-\d{4}-\d{4}	
IL\d{2}\d{4}\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{4}-\d{3}	
LT\d{2}\d{4}\d{4}\d{4}\d{4}	Lithuania patterns
LT\d{2} \d{4} \d{4} \d{4} \d{4}	
LT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	

**Table 30-55** IBAN East wide breadth patterns (*continued*)

Pattern	Description
LV\d{2}[A-Z]{4}\w{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{4}-\w	
ME\d{2}\d{4}\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{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\d{2}	
PL\d{2}\d{4}\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} \d{4}	
PL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
RO\d{2}[A-Z]{4}\w{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}-\w{4}	
RS\d{2}\d{4}\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{4}-\d{2}	
SI\d{2}\d{4}\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} \d{4}	
SK\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
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}-\d{4}	

**Table 30-55** IBAN East wide breadth patterns (*continued*)

Pattern	Description
TR\d{2}\d{4}\d\w{3}\w{4}\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}	

**Table 30-56** IBAN East wide breadth validator

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

## IBAN West system data identifier

The International Bank Account Number (IBAN) is an international standard for identifying bank accounts across national borders.

The IBAN West system 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 system data identifier detects a country-specific IBAN number that passes a checksum. IBAN numbers can include space delimiters, dash delimiters, or no delimiters.

**Table 30-57** IBAN West wide breadth patterns

Pattern	Description
DK\d{2}\d{4}\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}-\d{2}	
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}\d{4}	
ES\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	
FI\d{2}\d{4}\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}	

**Table 30-57** IBAN West wide breadth patterns (*continued*)

Pattern	Description
FO\d{2}\d{4}\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{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{4}\d{2}	United Kingdom
GB\d{2} [A-Z]{4} \d{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{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{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{4}-\d{2}	
IE\d{2}[A-Z]{4}\d{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{4}\d{2}	Iceland patterns
IS\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{2}	
IS\d{2}-\d{4}-\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{4}-\d{2}	
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}	

**Table 30-57** IBAN West wide breadth patterns (*continued*)

Pattern	Description
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	
PT\d{2}-\d{4}-\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}-\d{4}	

**Table 30-58** IBAN West wide breadth patterns

Validator	Description
Mod 97 Validator	Computes the ISO 7064 Mod 97-10 checksum of the complete match.

## IP Address system data identifier

An IP address is the computer networking code that is used to identify devices and facilitate communications.

The IP Address system data identifier detects IP addresses.

This data identifier offers three breadths of detection:

- Wide  
See “[IP Address wide breadth](#)” on page 570.
- Medium  
See “[IP Address medium breadth](#)” on page 571.
- Narrow  
See “[IP Address narrow breadth](#)” on page 572.

### IP Address wide breadth

The wide 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.

**Table 30-59** IP Address wide breadth patterns

Pattern
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?</code>

**Table 30-60** 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.

**Table 30-61** IP Address medium breadth patterns

Pattern
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[0-9]</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[1-2][0-9]?</code>
<code>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?</code>

**Table 30-62** 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 30-63** 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}.\d{1,3}/[1-2][0-9]?
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}/[3][0-2]?

**Table 30-64** 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) system 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 system 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 556.

- The medium breadth restricts the patterns for detecting the numbers.  
 See “[Drivers License Number- FL, MI, MN States medium breadth](#)” on page 556.
- The narrow breadth requires a keyword match.  
 See “[Drivers License Number- FL, MI, MN States medium breadth](#)” on page 556.

## National Drug Code (NDC) wide breadth

The wide breadth edition of the National Drug Code (NDC) system 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 30-65** National Drug Code (NDC) wide breadth patterns

Patterns
*?\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) system 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 30-66** 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) system 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 30-67** National Drug Code (NDC) narrow 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}

**Table 30-68** 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 system 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 system data identifier detects the presence of this 18-digit number.

The wide breadth edition of the People's Republic of China ID system data identifier detects an 18-digit number with the last number being used to validate a checksum.

**Table 30-69** People's Republic of China ID wide breadth patterns

Pattern
<code>\d{17}[Xx]</code>
<code>\d{18}</code>

**Table 30-70** 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.

# Singapore NRIC system data identifier

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 system data identifier detects 9 characters in the pattern LDDDDDDDL. The last character is used to validate a checksum.

**Table 30-71** Singapore NRIC wide breadth pattern

Pattern
<code>[SFTGsftg]\d{7}\w</code>

**Table 30-72** 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 system 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 system 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 576.
- The medium breadth edition matches a dash-delimited number only.  
See [“South Korea Resident Registration Number medium breadth”](#) on page 577.

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 system 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 30-73** South Korea Resident Registration Number wide breadth patterns

Pattern
<code>\d{2}[01]\d[0123]\d{8}</code>
<code>\d{2}[01]\d[0123]\d-\d{7}</code>

**Table 30-74** South Korea Resident Registration Number wide breadth validators

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 system 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 30-75** South Korea Resident Registration Number medium breadth pattern

Pattern
<code>\d\d[01]\d[0123]\d-\d{7}</code>

**Table 30-76** South Korea Resident Registration Number medium breadth 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 system 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 system 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 30-77** Spanish DNI ID wide breadth patterns

Pattern
<code>\d{8}-\w</code>
<code>X-\d{8}-\w</code>

**Table 30-78** 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 system 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 system 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 578.
- Narrow breadth  
See [“SWIFT Code narrow breadth”](#) on page 579.

### SWIFT Code wide breadth

The wide breadth edition of the SWIFT Code system 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 30-79** SWIFT Code wide breadth patterns

Pattern
[A-Z]{6}\w{2}
[A-Z]{6}\w{5}

**Table 30-80** SWIFT Code wide breadth validators

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, iso9362, swift, swift#, swiftcode, swiftnumber, swiftroutingnumber.

## SWIFT Code narrow breadth

The narrow breadth edition of the SWIFT Code system 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 30-81** SWIFT Code narrow breadth patterns

Pattern
[A-Z]{6}\w{2}
[A-Z]{6}\w{5}

**Table 30-82** SWIFT Code narrow breadth validators

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.

**Table 30-82** SWIFT Code narrow breadth validators (*continued*)

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, iso9362, swift#, swiftcode, swiftnumber, swiftroutingnumber, swift code, swift number, swift routing number, bic number, bic code, bic #

## Swiss AHV Number system 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 system data identifier detects the 11-digit identifier with or without the standard period delimiter (DDD.DD.DDD.DDD) and is validated against a checksum algorithm.

**Table 30-83** Swiss AHV Number wide breadth patterns

Pattern
\d{8}-\w
X-\d{8}-\w

**Table 30-84** Swiss AHV Number wide breadth validators

Validator	Description
Swiss AHV	Swiss AHV Modulus 11 Checksum.
Number Delimiter	Validates a match by checking the surrounding numbers.

## Taiwan ROC ID system 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 ROC ID system 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 30-85** Taiwan ROC ID wide breadth pattern

Patterns
[A-Z][12][0-3]\d{7}
[A-Z][ABCD]\d{8}

**Table 30-86** Taiwan ROC ID wide breadth validator

Validator	Description
Taiwan ID	Taiwan ID checksum.

## UK Drivers License Number system 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 system 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 581.
- Medium  
See [“UK Drivers License Number medium breadth”](#) on page 582.
- Narrow  
See [“UK Drivers License Number narrow breadth”](#) on page 582.

### UK Drivers License Number wide breadth

The wide breadth edition of the UK Drivers License Number system 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 30-87** UK Drivers License Number wide breadth patterns

Pattern
<code>\w{5}\d{0156}\d{4}\w{3}\l{2}</code>
<code>\w{5} \d{0156}\d{4} \w{3}\l{2}</code>

## UK Drivers License Number medium breadth

The medium breadth edition of the UK Drivers License Number system 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 30-88** UK Drivers License Number medium breadth patterns

Pattern
<code>\w{5}\d{0156}\d{4}\w{3}\l{2}</code>
<code>\w{5} \d{0156}\d{4} \w{3}\l{2}</code>

**Table 30-89** 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 system 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 30-90** UK Drivers License Number narrow breadth patterns

Pattern
<code>\w{5}\d[0156]\d{4}\w{3}\l{2}</code>
<code>\w{5} \d[0156]\d{4} \w{3}\l{2}</code>

**Table 30-91** 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
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 system 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 Drivers License Number system 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 30-92** UK Electoral Roll Number wide breadth pattern

Pattern
<code>\l{2,3}\d{1,4}</code>

The wide breadth edition of the Electoral Roll Number system data identifier implements two validators to require the presence of an electoral number-related keyword and a UK-related keyword.

**Table 30-93** UK Electoral Roll Number wide breadth validators

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:  <b>electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoral roll#, electoral#, electoralnumber, electoralroll#, electoralrollno</b>
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:  <b>british, the united kingdom, uk, united kingdom, unitedkingdom</b>

## UK National Health Service (NHS) Number system 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 system 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 585.
- **Narrow**  
 See [“UK National Health Service \(NHS\) Number narrow breadth”](#) on page 585.

---

**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 system 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 30-94** UK National Health Service (NHS) Number medium breadth patterns

Pattern	Description
<code>\d{3}.\d{3}.\d{4}</code>	Pattern for detecting the format DDD-DDD-DDDD separated by periods.
<code>\d{3} \d{3} \d{4}</code>	Pattern for detecting the format DDD-DDD-DDDD separated by spaces.
<code>\d{3}-\d{3}-\d{4}</code>	Pattern for detecting the format DDD-DDD-DDDD separated by dashes.

The medium breadth edition of the UK National Health Service (NHS) Number system 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 30-95** 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: <b>national health service, NHS</b>

## UK National Health Service (NHS) Number narrow breadth

The narrow breadth edition of the UK National Health Service (NHS) Number system data identifier implements patterns to detect numbers in the currently defined format: DDD-DDD-DDDD (where D is a digit), separated with dashes, spaces, or periods.

**Table 30-96** 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 system 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 30-97** 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:  <b>national health service, NHS</b>
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match:  <b>uk, united kingdom, britain, england, gb</b>

## UK National Insurance Number system 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 system 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 587.
- Medium  
See “UK National Insurance Number medium breadth” on page 587.
- Narrow  
See “UK National Insurance Number narrow breadth” on page 588.

## UK National Insurance Number wide breadth

The wide breadth edition of the UK National Insurance Number system data identifier implements patterns to detect 9-digit numbers of the format LL 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 30-98** 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.
[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 system data identifier implements patterns to detect 9-digit numbers of the format LL 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 30-99** 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 system 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 30-100** 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} [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 system data identifier implements a validator that requires the presence of a national insurance-related keyword.

**Table 30-101** 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:  <b>insurance no., insurance number, insurance#, insurancenum, national insurance number, nationalinsurance#, nationalinsurancenum, nin, nino</b>

# UK Passport Number system 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 system 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 589.
- Medium  
See “[UK Passport Number medium breadth](#)” on page 589.
- Narrow  
See “[UK Passport Number narrow breadth](#)” on page 590.

## UK Passport Number wide breadth

The wide breadth edition of the UK Passport Number system data identifier implements a pattern to detect 9-digit numbers.

---

**Note:** The wide breadth edition of the UK Passport Number system data identifier does not include any validators.

---

**Table 30-102** UK Passport Number wide breadth pattern

Pattern	Description
<code>\d{9}</code>	Pattern for detecting 9-digit numbers.

## UK Passport Number medium breadth

The medium breadth edition of the UK Passport Number system data identifier implements a pattern to detect 9-digit numbers.

**Table 30-103** UK Passport Number medium breadth pattern

Pattern	Description
<code>\d{9}</code>	Pattern for detecting 9-digit numbers.

The medium breadth edition of the UK Passport Number system 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 30-104** 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:  <b>123456789</b>
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:  <b>passport, passport#, passportID, passportno, passportnumber</b>

## UK Passport Number narrow breadth

The narrow breadth edition of the UK Passport Number system data identifier implements a pattern to detect 9-digit numbers.

**Table 30-105** 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 system 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 30-106** 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:  <b>123456789</b>

**Table 30-106** UK Passport Number narrow breadth validators (*continued*)

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: <b>passport, passport#, passportID, passportno, passportnumber</b>
Find keywords: UK-related	At least one of the following keywords or key phrases must be present for the data to match: <b>uk, united kingdom, britain, england, gb</b>

## UK Tax ID Number system 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 system 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 591.
- Medium  
See “[UK Tax ID Number medium breadth](#)” on page 592.
- Narrow  
See “[UK Tax ID Number narrow breadth](#)” on page 592.

### UK Tax ID Number wide breadth

The wide breadth edition of the UK Tax ID Number system data identifier implements a single pattern to detect 10-digit numbers.

---

**Note:** The wide breadth edition of the UK Tax ID Number system data identifier does not include any validators.

---

**Table 30-107** UK Passport Number 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 system data identifier implements a single pattern to detect 10-digit numbers.

**Table 30-108** 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 system data identifier implements two validators: one to eliminate common test numbers, such as 1234567890, and another to eliminate numbers with all the same digit.

**Table 30-109** 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:  <b>0123456789, 1234567890, 9876543210, 0987654321</b>

## UK Tax ID Number narrow breadth

The narrow breadth edition of the UK Tax ID Number system data identifier implements a single pattern to detect 10-digit numbers.

**Table 30-110** 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 system data identifier implements three validators: one to eliminate 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.

**Table 30-111** UK Tax ID Number narrow 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:  <b>0123456789, 1234567890, 9876543210, 0987654321</b>
Find keywords: Tax ID-related	At least one of the following keywords or key phrases must be present for the data to match:  <b>tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax#, taxid#</b>

## US Individual Tax Identification Number (ITIN) system data identifier

The US Individual Tax Identification Number (ITIN) is used for tax processing number and 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) system 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 594.
- **Medium**  
See [“US Individual Tax Identification Number \(ITIN\) medium breadth”](#) on page 594.
- **Narrow**  
See [“US Individual Tax Identification Number \(ITIN\) narrow breadth”](#) on page 595.

## US Individual Tax Identification Number (ITIN) wide breadth

The wide breadth edition of the US Individual Tax Identification Number (ITIN) system 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) system data identifier does not include any validators.

---

**Table 30-112** 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) system data identifier implements patterns to detect 9-digit numbers with the pattern DDD-DD-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 30-113** 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) system data identifier implements a single validator to check the surrounding characters.

**Table 30-114** 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) system 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 30-115** 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) system 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.

**Table 30-116** US Individual Tax Identification Number (ITIN) narrow breadth 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.
Find keywords: ITIN-related	At least one of the following keywords or key phrases must be present for the data to be matched.  <b>individual taxpayer identification number, itin, i.t.i.n.</b>

## US Social Security Number (SSN) system data identifier

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) system 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 596.
- Medium  
See [“US Social Security Number \(SSN\) medium breadth”](#) on page 598.
- Narrow  
See [“US Social Security Number \(SSN\) narrow breadth”](#) on page 599.

### US Social Security Number (SSN) wide breadth

The wide breadth edition of the US Social Security Number (SSN) system 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 30-117** Social Security Number (SSN) wide breadth patterns

Pattern	Description
<code>\d{3}-\d{2}-\d{4}</code>	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
<code>\d{3}.\d{2}.\d{4}</code>	Matches the SSN format delimited by periods.
<code>\d{3} \d{2} \d{4}</code>	Matches the SSN format delimited by spaces.
<code>\d{3} \\ \d{2} \\ \d{4}</code>	Matches the SSN format delimited by backslashes.
<code>\d{3} / \d{2} / \d{4}</code>	Matches the SSN format delimited by forward slashes.
<code>\d{9}</code>	Matches any 9-digit number that is not delimited.

The wide breadth edition of the US Social Security Number (SSN) system 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 30-118** 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).

**Table 30-118** Social Security Number (SSN) wide breadth validators (*continued*)

Validator	Description
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) system data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods.

**Table 30-119** Social Security Number (SSN) medium breadth patterns

Pattern	Description
<code>\d{3}-\d{2}-\d{4}</code>	Matches the standard SSN format, which is any three digits followed by a hyphen, two digits, a hyphen, and any four digits.
<code>\d{3}.\d{2}.\d{4}</code>	Matches the SSN format delimited by periods.
<code>\d{3} \d{2} \d{4}</code>	Matches the SSN format delimited by spaces.

The medium breadth edition of the US Social Security Number (SSN) system 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 30-120** 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).

**Table 30-120** Social Security Number (SSN) medium breadth validators (*continued*)

Validator	Description
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) system data identifier implements patterns to detects 9-digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators.

**Table 30-121** 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) system 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.

**Table 30-122** Social Security Number (SSN) narrow breadth validators

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).

**Table 30-122** Social Security Number (SSN) narrow breadth validators (*continued*)

Mandatory Validator	Description
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:  <b>social security number, ssn, ss#</b>

# 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.

EDM Rule

**Patient Data and Drug Keywords**

This compound rule looks for any match of the following data in combination with a keyword from the "Prescription Drug Names" dictionary. Both conditions must be satisfied for the rule to trigger an incident.

- UK NIN (National Insurance Number)
- Account number
- Last name
- ID card number
- Email
- Phone
- UK NHS (National Health Service) number

EDM Rule

**Patient Data and Disease Keywords**

This compound rule looks for any match of the following data in combination with a keyword from the "Disease Names" dictionary. Both conditions must be satisfied for the rule to trigger an incident.

- UK NIN (National Insurance Number)
- Account number
- Last name
- ID card number
- Email
- Phone
- UK NHS (National Health Service) number

EDM Rule

**Patient Data and Treatment Keywords**

This compound rule looks for any match of the following data in combination with a keyword from the "Medical Treatment Keywords" dictionary. Both conditions must be satisfied for the rule to trigger an incident:

- UK NIN (National Insurance Number)
- Account number
- Last name
- ID card number
- Email
- Phone
- UK NHS (National Health Service) number

DCM Rule	<b>UK NHS Number and Drug Keywords</b>  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.
DCM Rule	<b>UK NHS Number and Disease Keywords</b>  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.
DCM Rule	<b>UK NHS Number and Treatment Keywords</b>  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.

See ["Choosing an Exact Data Profile"](#) on page 333.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## Canadian Social Insurance Numbers policy template

This policy detects patterns indicating Canadian social insurance numbers (SINs) at risk of exposure.

DCM Rule	<b>Canadian Social Insurance Numbers</b>  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 338.

See ["Exporting policy detection as a template"](#) on page 362.

## 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.

**Table 31-1** Detection exception: Exclude emails that contain the mandated keywords

Method	Condition	Configuration
Simple exception	Content Matches Keyword (DCM)	<p>Exclude emails that contain the mandated keywords (Keyword Match):</p> <ul style="list-style-type: none"> <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> </ul> <p><b>Note:</b> After you define the keywords, you can choose to count all matches and require 2 keywords from the list to be matched.</p>

The detection exception **CAN-SPAM Compliant Emails** excludes from detection document content from the selected IDM index with at least 100% match.

**Table 31-2** Detection exception: CAN-SPAM Compliant Emails

Method	Condition	Configuration
Simple exception	Content Matches Document Profile (IDM)	<p>Exception for CAN-SPAM compliant emails (IDM):</p> <ul style="list-style-type: none"> <li>■ Exact content match (100%)</li> <li>■ Look in the message body and attachments.</li> <li>■ Check for existence.</li> </ul> <p>See <a href="#">"Choosing an Indexed Document Profile"</a> on page 334.</p>

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.

**Table 31-3** Detection rule: Monitor Email From Bulk Mailer

Method	Condition	Configuration
Simple rule	Sender/User Matches Pattern (DCM)	Monitor Email From Bulk Mailer (Sender): <ul style="list-style-type: none"> <li>■ Match sender pattern(s): [bulk-mailer@company.com] (user defined)</li> <li>■ Severity: High.</li> </ul>

See [“Creating a policy from a template”](#) on page 321.

See [“Exporting policy detection as a template”](#) on page 362.

## 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      **Forbidden Websites 2**  
 This rule looks for a match of a specified URL in the "Forbidden Websites 2" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

# Confidential Documents policy template

This policy detects company-confidential documents at risk of exposure.

IDM Rule	<b>Confidential Documents, Indexed</b>  This rule looks for content from specific documents registered as confidential; returns a match if 80% or more of the source document is found.
DCM Rule	<b>Confidential Documents</b>  This rule is a compound rule with two conditions; both must be met for the rule to trigger an incident. This rule looks for a combination of keywords from the "Confidential Keywords" dictionary and the following file types: <ul style="list-style-type: none"><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><li>■ doc</li><li>■ pdf</li><li>■ ppt</li></ul>
DCM Rule	<b>Proprietary Documents</b>  This compound rule looks for a combination of keywords from the "Proprietary Keywords" dictionary and the above referenced file types.
DCM Rule	<b>Internal Use Only Documents</b>  This compound rule looks for a combination of keywords from the "Internal Use Only Keywords" dictionary and the above referenced file types.
DCM Rule	<b>Documents Not For Distribution</b>  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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## Customer Data Protection policy template

This policy detects customer data at risk of exposure.

EDM Rule

### **Username/Password Combinations**

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

EDM Rule	<p><b>Date of Birth</b></p> <p>This rule looks for any three of the following data fields in combination:</p> <ul style="list-style-type: none"><li>■ SSN</li><li>■ Phone</li><li>■ Email</li><li>■ First Name</li><li>■ Last Name</li><li>■ Bank Card number</li><li>■ Account Number</li><li>■ ABA Routing Number</li><li>■ Canadian Social Insurance Number</li><li>■ UK National Insurance Number</li><li>■ Date of Birth</li></ul> <p>However, the following combinations are not a violation:</p> <ul style="list-style-type: none"><li>■ Phone, email, and first name</li><li>■ Phone, email, and last name</li><li>■ Email, first name, and last name</li><li>■ Phone, first name, and last name</li></ul>
EDM Rule	<p><b>Exact SSN or CCN</b></p> <p>This rule looks for an exact social security number or bank card number.</p>
EDM Rule	<p><b>Customer Directory</b></p> <p>This rule looks for Phone or Email.</p>
DCM Rule	<p><b>US Social Security Number Patterns</b></p> <p>This rule looks for a match to the Social Security number data identifier and a keyword from the "US SSN Keywords" dictionary.</p>
DCM Rule	<p><b>Credit Card Numbers, All</b></p> <p>This rule looks for a match to the credit card number system pattern and a keyword from the "Credit Card Number Keywords" dictionary.</p>
DCM Rule	<p><b>ABA Routing Numbers</b></p> <p>This rule looks for a match to the ABA Routing number data identifier and a keyword from the "ABA Routing Number Keywords" dictionary.</p>

See [“About implementing Exact Data Matching”](#) on page 368.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-4** UK Data Protection Act, Personal Data detection rule

Description	
<p>This EDM rule looks for three of the following columns of data:</p> <ul style="list-style-type: none"> <li>■ NIN (National Insurance Number)</li> <li>■ Account number</li> <li>■ Pin</li> <li>■ Bank card number</li> <li>■ First name</li> <li>■ Last name</li> <li>■ Drivers license</li> <li>■ Password</li> <li>■ Tax payer ID</li> <li>■ UK NHS number</li> <li>■ Date of birth</li> <li>■ Mother's maiden name</li> <li>■ Email address</li> <li>■ Phone number</li> </ul>	<p>However, the following combinations are not an incident:</p> <ul style="list-style-type: none"> <li>■ First name, last name, pin</li> <li>■ First name, last name, password</li> <li>■ First name, last name, email</li> <li>■ First name, last name, phone</li> <li>■ First name, last name, mother's maiden name</li> </ul>

**Table 31-5** Additional detection rules in the Data Protection Act 1998 policy template

Description
<p>The <b>UK Electoral Roll Numbers</b> rule implements the UK Electoral Roll Number data identifier.</p> <p>See <a href="#">“UK Electoral Roll Number system data identifier”</a> on page 583.</p>
<p>The <b>UK National Insurance Numbers</b> rule implements the narrow breadth edition of the UK National Insurance Number data identifier.</p> <p>See <a href="#">“UK National Insurance Number system data identifier”</a> on page 586.</p>

**Table 31-5** Additional detection rules in the Data Protection Act 1998 policy template (*continued*)

Description
The <b>UK Tax ID Numbers</b> rule implements the narrow edition of the UK Tax ID Number data identifier. See <a href="#">“UK Tax ID Number system data identifier”</a> on page 591.
The <b>UK Drivers License Numbers</b> rule implements the narrow breadth edition of the UK Driver's License number data identifier. See <a href="#">“UK Drivers License Number system data identifier”</a> on page 581.
The <b>UK Passport Numbers</b> rule implements the narrow breadth edition of the UK Passport Number data identifier. See <a href="#">“UK Passport Number system data identifier”</a> on page 589.
The <b>UK NHS Numbers</b> rule implements the narrow breadth edition of the UK National Health Service (NHS) Number data identifier. See <a href="#">“UK National Health Service (NHS) Number system data identifier”</a> on page 584.
See <a href="#">“Choosing an Exact Data Profile”</a> on page 333. See <a href="#">“Configuring policies”</a> on page 338. See <a href="#">“Exporting policy detection as a template”</a> on page 362.

## 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.

## EDM Rule

**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

## EDM Rule

**EU Data Protection, Contact Info**

This rule looks for any two of the following data columns: last name, phone, account number, username, and email.

## Exception

**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 333.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

# 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.

**Table 31-6** Detection rule: Top Secret Information (Keyword Match)

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Top Secret Information (Keyword Match): <ul style="list-style-type: none"> <li>■ Keyword dictionary: "TOP SECRET//"</li> <li>■ Severity: High</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole or partial words.</li> </ul>

The detection rule **Secret Information** (Keyword Match) looks for any keywords in the "Secret Information" dictionary.

**Table 31-7** Detection rule: Secret Information (Keyword Match)

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Secret Information (Keyword Match): <ul style="list-style-type: none"> <li>■ Keyword dictionary: "SECRET//"</li> <li>■ Severity: High</li> <li>■ Check for existence</li> <li>■ Look in envelope, subject, body, attachments</li> <li>■ Case sensitive</li> <li>■ Match on whole or partial words.</li> </ul>

The detection rule **Classified or Restricted Information** (Keyword Match) looks for any keywords in the "Classified or Restricted Information" dictionary.

**Table 31-8** Detection rule: Classified or Restricted Information (Keyword Match)

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Classified or Restricted Information (Keyword Match): <ul style="list-style-type: none"> <li>■ Keyword dictionary: "CLASSIFIED///RESTRICED///"</li> <li>■ Severity: High</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole or partial words.</li> </ul>

The detection rule **Other Sensitive Information** looks for any keywords in the "Other Sensitive Information" dictionary.

**Table 31-9** Other Sensitive Information detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Other Sensitive Information (Keyword Match): <ul style="list-style-type: none"> <li>■ Keyword dictionary: FOR OFFICIAL USE ONLY, SENSITIVE BUT UNCLASSIFIED,DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION</li> <li>■ Severity: High</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole words only.</li> </ul>

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 334.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## Employee Data Protection policy template

This policy detects employee data at risk of exposure.

EDM Rule

### **Username/Password Combinations**

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

EDM Rule

### **Employee Directory**

This rule looks for Phone or Email.

DCM Rule	<b>US Social Security Number Patterns</b> This rule looks for a match to the Social Security number data identifier and a keyword from the "US SSN Keywords" dictionary.
DCM Rule	<b>Credit Card Numbers, All</b> This rule looks for a match to the credit card number system pattern and a keyword from the "Credit Card Number Keywords" dictionary.
DCM Rule	<b>ABA Routing Numbers</b> This rule looks for a match to the ABA Routing number data identifier and a keyword from the "ABA Routing Number Keywords" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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	<b>Password Protected Files</b> This rule looks for the following file types: encrypted_zip, encrypted_doc, encrypted_xls, or encrypted_ppt.
DCM Rule	<b>PGP Files</b> This rule looks for the following file type: pgp.
DCM Rule	<b>GPG Files</b> This rule looks for a keyword from the "GPG Encryption Keywords" dictionary.
DCM Rule	<b>S/MIME</b> This rule looks for a keyword from the "S/MIME Encryption Keywords" dictionary.
DCM Rule	<b>HushMail Transmissions</b> This rule looks for a match from a list of recipient URLs.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

# 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 31-10** Detection rule: Indexed EAR Commerce Control List Items and Recipients

Method	Condition	Configuration
Compound rule	Content Matches Exact Data (EDM)	See <a href="#">"Choosing an Exact Data Profile"</a> on page 333.
	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 31-11** Detection rule: EAR Commerce Control List and Recipients

Method	Condition	Configuration
Compound rule	Recipient Matches Pattern (DCM)	EAR Commerce Control List and Recipients (Recipient): <ul style="list-style-type: none"> <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): <ul style="list-style-type: none"> <li>■ Match: EAR CCL Keywords</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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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.

**Table 31-12** Username/Password Combinations detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	<p>This condition detects exact data containing both of the following data items:</p> <ul style="list-style-type: none"> <li>■ User name</li> <li>■ Password</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

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 31-13** Exact SSN or CCN detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	<p>This condition detects exact data containing either of the following data columns:</p> <ul style="list-style-type: none"> <li>■ Social security number (Taxpayer ID)</li> <li>■ Bank Card Number</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

The **Customer Directory** detection rule detects the presence of either an email address or a phone number from a profiled database.

**Table 31-14** Customer Directory detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	<p>This condition detects exact data containing either of the following data columns:</p> <ul style="list-style-type: none"> <li>■ Email address</li> <li>■ Phone number</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

The **Three or More Data Columns** detection rule detects exact data containing three or more of data items from a profiled database index.

**Table 31-15**      Three or More Data Columns detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	<p>Detects exact data containing three or more of the following data items:</p> <ul style="list-style-type: none"> <li>■ ABA Routing Number</li> <li>■ Account Number</li> <li>■ Bank Card Number</li> <li>■ Birth Date</li> <li>■ Email address</li> <li>■ First Name</li> <li>■ Last Name</li> <li>■ National Insurance Number</li> <li>■ Password</li> <li>■ Phone Number</li> <li>■ Social Insurance Number</li> <li>■ Social security number (Taxpayer ID)</li> <li>■ User name</li> </ul> <hr/> <p>However, the following combinations are not a match:</p> <ul style="list-style-type: none"> <li>■ Phone Number, Email, First Name</li> <li>■ Phone Number, First Name, Last Name</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

The **US Social Security Number Patterns** detection rule implements the narrow breadth edition of the US Social Security Number (SSN) system Data Identifier.

See [“US Social Security Number \(SSN\) system data identifier”](#) on page 596.

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.

**Table 31-16** US Social Security Number Patterns detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul style="list-style-type: none"> <li>■ Data Identifier: US Social Security Number (SSN) narrow breadth See <a href="#">“US Social Security Number (SSN) narrow breadth”</a> on page 599.</li> <li>■ Severity: High.</li> <li>■ Count all matches.</li> <li>■ Look in envelope, subject, body, attachments.</li> </ul>

The **Credit Card Numbers, All** detection rule implements the narrow breadth edition of the Credit Card Number system Data Identifier.

See [“Credit Card Number system data identifier”](#) on page 546.

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.

**Table 31-17** Credit Card Numbers, All detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul style="list-style-type: none"> <li>■ Data Identifier: Credit Card Number narrow breadth See <a href="#">“Credit Card Number narrow breadth”</a> on page 549.</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 system data identifier”](#) on page 536.

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.

**Table 31-18** ABA Routing Numbers detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<ul style="list-style-type: none"> <li>■ Data Identifier: ABA Routing Number narrow breadth See <a href="#">“ABA Routing Number narrow breadth”</a> on page 538.</li> <li>■ Severity: High.</li> <li>■ Count all matches.</li> <li>■ Look in envelope, subject, body, attachments.</li> </ul>

See [“Creating a policy from a template”](#) on page 321.

See [“Exporting policy detection as a template”](#) on page 362.

## Financial Information policy template

The Financial Information policy detects financial data and information.

IDM Rule	<p><b>Financial Information, Indexed</b></p> <p>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.</p>
DCM Rule	<p><b>Financial Information</b></p> <p>This rule looks for the combination of specified file types, keywords from the "Financial Keywords" dictionary, and keywords from the "Confidential/Proprietary Words" dictionary.</p> <p>The specified file types are as follows:</p> <ul style="list-style-type: none"> <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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

# Forbidden Websites policy template

The Forbidden Websites policy detects access to specified Web sites.

DCM Rule                    **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

- 1    Configure your web proxy server to forward GET requests to the Network Prevent (Web) server.
- 2    Set the L7.processGets Advanced setting on the Network Prevent (Web) server to "true" (which is the default).
- 3    Reduce the L7.minSizeofGetURL Advanced setting on the Network Prevent (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 the server's 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.

---

- 4    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 338.

See ["Exporting policy detection as a template"](#) on page 362.

# Gambling policy template

This policy detects any reference to gambling.

DCM Rule                    **Suspicious Gambling Keywords**

This rule looks for five instances of keywords from the "Gambling Keywords, Confirmed" dictionary.

DCM Rule

**Less Suspicious Gambling Keywords**

This rule looks for 10 instances of keywords from the "Gambling Keywords, Suspect" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-19** Gramm-Leach-Bliley detection methods

Detection method	Type	Description
Username/Password Combinations	Simple rule: EDM	This rule looks for user names and passwords in combination.  See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.
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.

**Table 31-19** Gramm-Leach-Bliley detection methods (*continued*)

Detection method	Type	Description
3 or more critical customer fields	Simple rule: EDM	<p>This rule looks for a match among any three of the following fields:</p> <ul style="list-style-type: none"> <li>■ Account number</li> <li>■ Bank card number</li> <li>■ Email address</li> <li>■ First name</li> <li>■ Last name</li> <li>■ PIN number</li> <li>■ Phone number</li> <li>■ Social security number</li> <li>■ ABA Routing Number</li> <li>■ Canadian Social Insurance Number</li> <li>■ UK National Insurance Number</li> <li>■ Date of Birth</li> </ul> <p>However, the following combinations are not a match:</p> <ul style="list-style-type: none"> <li>■ Phone, email, and first name</li> <li>■ Phone, email, and last name</li> <li>■ Email, first name, and last name</li> <li>■ Phone, first name, and last name</li> </ul>
ABA Routing Numbers	Simple rule: DCM (DI)	<p>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.</p> <p>See <a href="#">“ABA Routing Number narrow breadth”</a> on page 538.</p>

**Table 31-19**      Gramm-Leach-Bliley detection methods (*continued*)

Detection method	Type	Description
US Social Security Numbers	Simple rule: DCM (DI)	<p>This rule looks for social security numbers. For this rule to match, there must be a number that fits the US SSN regular expression pattern. 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.</p> <p>See <a href="#">"US Social Security Number (SSN) narrow breadth"</a> on page 599.</p>
Credit Card Numbers	Simple rule: DCM (DI)	<p>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:</p> <ul style="list-style-type: none"> <li>■ American Express</li> <li>■ Diner's Club</li> <li>■ Discover</li> <li>■ Japan Credit Bureau (JCB)</li> <li>■ MasterCard</li> <li>■ Visa</li> </ul> <p>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.</p> <p>See <a href="#">"Credit Card Number narrow breadth"</a> on page 549.</p>

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## 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 PHI.

This policy template detects data concerning prescription drugs, diseases, and treatments in combination with Protected Health Information (PHI). Organizations that are not subject to HIPAA can also use this policy to control PHI data.

TPOs (Treatment, Payment, or health care Operations) are service providers to health care organizations and have an exception for HIPAA information restrictions. This policy does not trigger an incident if the protected information is sent to one of the allowed partners.

The [Table 31-20](#) is evaluated before any detection rules. The template requires that you enter the allowed email addresses.

**Table 31-20** TPO detection exception

Method and cardinality	Condition type	Configuration
Simple detection exception	Content Matches Keyword (DCM)	Looks for a recipient email address matching one from the "TPO Email Addresses" keyword dictionary.

The [Table 31-21](#) looks for a match against any single column from a profiled Patient Data database record.

**Table 31-21** Patient Data detection rule

Method and cardinality	Condition type	Configuration
Simple detection rule	Content Matches Exact Data (EDM)	Patient Data (EDM): <ul style="list-style-type: none"> <li>■ Last name</li> <li>■ Tax payer ID (SSN)</li> <li>■ Email address</li> <li>■ Account number</li> <li>■ ID card number</li> <li>■ Phone number</li> </ul> See " <a href="#">Choosing an Exact Data Profile</a> " on page 333.

The [Table 31-22](#) requires a Patient Data condition match and a match from the "Drug Code" data identifier.

**Table 31-22** Patient Data and Drug Codes detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Exact Data (EDM)	Looks for a match against any single column from a profiled Patient Data database record.
	Content Matches Data Identifier	See <a href="#">“National Drug Code (NDC) system data identifier”</a> on page 572.

The [Table 31-23](#) requires a Patient Data condition match in combination with a keyword from the "Prescription Drug Names" keyword dictionary.

**Table 31-23** Patient Data and Prescription Drug Names detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Exact Data (EDM)	Looks for a match against any single column from a profiled Patient Data database record.
	Content Matches Keyword (DCM)	

The [Table 31-24](#) requires a Patient Data condition match in combination with a keyword from the "Medical Treatment Keywords" keyword dictionary.

**Table 31-24** Patient Data and Treatment Keywords detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Exact Data (EDM)	Looks for a match against any single column from a profiled Patient Data database record.
	Content Matches Keyword (DCM)	

The [Table 31-25](#) requires a Patient Data condition match in combination with a keyword from the "Disease Names" keyword dictionary.

**Table 31-25** Patient Data and Disease Keywords detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Exact Data (EDM)	Looks for a match against any single column from a profiled Patient Data database record.
	Content Matches Keyword (DCM)	

The [Table 31-26](#) looks for a social security number using the US Social Security Number (SSN) system Data Identifier (narrow breadth) and for a keyword from the "Prescription Drug Names" keyword dictionary.

**Table 31-26** SSN and Drug Keywords detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Data Identifier	US Social Security Number (SSN) system Data Identifier (narrow breadth)  See <a href="#">"US Social Security Number (SSN) system data identifier"</a> on page 596.
	Content Matches Keyword	"Prescription Drug Names" keyword dictionary

The [Table 31-27](#) rule looks for the social security number using the US SSN system Data Identifier (narrow breadth) and for a match from the "Medical Treatment Keywords" keyword dictionary.

**Table 31-27** SSN and Treatment Keywords detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Data Identifier	US Social Security Number (SSN) system Data Identifier (narrow breadth)  See <a href="#">"US Social Security Number (SSN) system data identifier"</a> on page 596.
	Content Matches Keyword	"Medical Treatment Keywords" keyword dictionary

The [Table 31-28](#) rule looks for the social security number using the US SSN system Data Identifier (narrow breadth) and for a match from the "Disease Names" keyword keyword dictionary.

**Table 31-28** SSN and Disease Keywords detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Data Identifier	US Social Security Number (SSN) system Data Identifier (narrow breadth)  See <a href="#">"US Social Security Number (SSN) system data identifier"</a> on page 596.
	Content Matches Keyword	"Disease Names" keyword keyword dictionary

The [Table 31-29](#) rule looks for the social security number using the US SSN system Data Identifier (narrow breadth) and for a drug code using the Drug Code system Data Identifier (narrow breadth).

**Table 31-29** SSN and Drug Code detection rule

Method and cardinality	Condition type	Configuration
Compound detection rule	Content Matches Data Identifier	US SSN system Data Identifier (narrow breadth)  See <a href="#">"US Social Security Number (SSN) system data identifier"</a> on page 596.
	Content Matches Keyword	Drug Code system Data Identifier (narrow breadth)  See <a href="#">"National Drug Code (NDC) system data identifier"</a> on page 572.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## 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	<b>UK Data Protection Act, Personal Data</b>  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	<b>UK Electoral Roll Numbers</b>  This rule looks for a single compound condition with four parts: <ul style="list-style-type: none"><li>■ A single keyword from the "UK Keywords" dictionary</li><li>■ A pattern matching that of the UK Electoral Roll Number data identifier</li><li>■ A single keyword from the "UK Electoral Roll Number Words" dictionary</li><li>■ A single keyword from the "UK Personal Data Keywords" dictionary</li></ul>

See ["Choosing an Exact Data Profile"](#) on page 333.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## Illegal Drugs policy template

This policy detects conversations about illegal drugs and controlled substances.

DCM Rule	<b>Street Drugs</b>  This rule looks for five instances of keywords from the "Street Drug Names" dictionary.
DCM Rule	<b>Mass Produced Controlled Substances</b>  This rule looks for five instances of keywords from the "Manufactured Controlled Substances" dictionary.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

# 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 Rules**                      **ITIN**

This rule looks for a match to the US ITIN data identifier and a keyword from the "US ITIN Keywords" dictionary.

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

# 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 EDM file.

**Table 31-30**                      Indexed ITAR Munition Items and Recipients detection rule

Method	Conditions (both must match)	Configuration
Compound rule	Receipt Matches Pattern (DCM)	Match recipient email or URL domain from ITAR Country Codes list: <ul style="list-style-type: none"> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ At least 1 recipient(s) must match.</li> </ul>
	Content Matches Exact Data (EDM)	See <a href="#">"Choosing an Exact Data Profile"</a> on page 333.

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.

**Table 31-31** ITAR Munitions List and Recipients detection rule

Method	Conditions (both must match)	Configuration
Compound rule	Recipeint Matches Pattern (DCM)	Match recipient email or URL domain from ITAR Country Codes list: <ul style="list-style-type: none"> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ At least 1 recipient pattern must match.</li> </ul>
	Content Matches Keyword (DCM)	Match any keyword from the ITAR Munitions List: <ul style="list-style-type: none"> <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>■ Severity: High.</li> </ul>

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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
- riff
- macromedia\_dir
- midi
- mp3
- mpeg\_movie
- quickdraw
- realaudio
- wav
- video\_win
- vrmf

## DCM Rule

**Media Files Extensions**

This rule looks for file name extensions from the "Media Files Extensions" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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.

**Table 31-32** Merger and Acquisition Agreements compound detection rule

Condition	Configuration
Contract Specific Keywords (Keyword Match)	<ul style="list-style-type: none"> <li>■ Match any keyword: <b>merger, agreement, contract, letter of intent, term sheet, plan of reorganization</b></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 style="list-style-type: none"> <li>■ Match any keyword: <b>subsidiary, subsidiaries, affiliate, acquiror, merger sub, covenantor, acquired company, acquiring company, surviving corporation, surviving company</b></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>
Merger Consideration Keywords (Keyword Match)	<ul style="list-style-type: none"> <li>■ Match any keyword: <b>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</b></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 style="list-style-type: none"> <li>■ Match any keyword: <b>recitals, in witness whereof, governing law, Indemnify, Indemnified, indemnity, signature page, best efforts, gross negligence, willful misconduct, authorized representative, severability, material breach</b></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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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.

**Table 31-33** NASD Rule 2711 Documents, Indexed detection rule

Method	Condition	Configuration
Simple rule	Content Matches Document Signature (IDM)	NASD Rule 2711 Documents, Indexed (IDM): <ul style="list-style-type: none"> <li>■ Detect documents in selected Indexed Document Profile</li> <li>■ Require at least 80% content match.</li> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in body, attachments.</li> </ul> See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.

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.

**Table 31-34** NASD Rule 2711 and NYSE Rules 351 and 472 detection rule

Method	Condition	Configuration
Compound rule	Sender/User Matches Pattern (DCM)	NASD Rule 2711 and NYSE Rules 351 and 472 (Sender): <ul style="list-style-type: none"> <li>■ Match sender pattern(s) [research_analyst@company.com] (user defined)</li> <li>■ Severity: High.</li> <li>■ Matches on entire message.</li> </ul>
	Content Matches Keyword (DCM)	NASD Rule 2711 and NYSE Rules 351 and 472 (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "[company stock symbol]", "[name of offering company]", "[offering name (internal name)]".</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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-35** Stock Recommendation detection rule

Method	Conditions (all must match)	Configuration
Compound rule	Content Mathces Keyword (DCM)	Match keyword: "recommend" <ul style="list-style-type: none"> <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>
	Content Mathces Keyword (DCM)	Match keyword: "buy" or "sell" <ul style="list-style-type: none"> <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>
	Content Mathces Keyword (DCM)	Match keyword: "stock, stocks, security, securities, share, shares" <ul style="list-style-type: none"> <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>

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 31-36** NASD Rule 3010 and NYSE Rule 342 Keywords detection rule

Method	Conditions (both must match)	Configuration
Compound rule	Content Mathces Keyword (DCM)	Match keyword: "authorize", "discretion", "guarantee", "options" <ul style="list-style-type: none"> <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>
	Content Mathces Keyword (DCM)	Match keyword: "stock, stocks, security, securities, share, shares" <ul style="list-style-type: none"> <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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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.

**Table 31-37** Key Response Personnel detection rule

Detection method	Match condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	Match any three of the following data items: <ul style="list-style-type: none"> <li>■ First name</li> <li>■ Last name</li> <li>■ Phone</li> <li>■ Email</li> </ul> See <a href="#">"Choosing an Exact Data Profile"</a> on page 333.

**Table 31-38** Network Infrastructure Maps detection rule

Detection method	Match condition	Configuration
Simple rule	Content Matches Indexed Documents (IDM)	This rule requires an exact binary match. See <a href="#">"Choosing an Indexed Document Profile"</a> on page 334.

The Sensitive Keywords and Vulnerability Keywords detection rule looks for any keyword matches from the "Sensitive Keywords" dictionary and the "Vulnerability Keywords" dictionary.

**Table 31-39** Sensitive Keywords and Vulnerability Keywords detection rule

Detection method	Match conditions	Configuration
Compound rule	Content Matches Keyword (DCM)	Match any Sensitive Keyword: <ul style="list-style-type: none"> <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>
	Content Matches Keyword (DCM)	Match any Vulnerability Keyword: <ul style="list-style-type: none"> <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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

# 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 31-40** OFAC Special Designated Nationals List and Recipients detection rule

Method	Condition	Configuration
Compound rule	Recipient Matches Pattern (DCM)	OFAC Special Designated Nationals List and Recipients (Recipient): <ul style="list-style-type: none"> <li>■ Match e-mail or URL domain by OFAC SDN Country Code.</li> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ At least 1 recipient(s) must match.</li> <li>■ Matches on the entire message.</li> </ul>
	Content Matches Keyword (DCM)	Specially Designated Nationals List (Keyword Match): <ul style="list-style-type: none"> <li>■ Match keyword from the Specially Designated Nationals List.</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>

The Communications to OFAC countries detection rule looks for a recipient with a country code matching entries from the "OFAC Country Codes" list.

**Table 31-41** Communications to OFAC countries detection rule

Method	Condition	Configuration
Simple rule	Recipient Matches Pattern (DCM)	Communications to OFAC countries (Recipient): <ul style="list-style-type: none"> <li>■ Match e-mail or URL domain by OFAC Country Code.</li> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ At least 1 recipient(s) must match.</li> <li>■ Matches on the entire message.</li> </ul>

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

# 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 31-42** High Confidentiality Indicators detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword	High Confidentiality Indicators (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "(confidentiality, high)", "(confidentiality,high)"</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>

The Moderate Confidentiality Indicators detection rule looks for any keywords in the "Moderate Confidentiality" dictionary.

**Table 31-43** Moderate Confidentiality Indicators detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword	Moderate Confidentiality Indicators (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "(confidentiality, moderate)", "(confidentiality,moderate)"</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>

The Low Confidentiality Indicators detection rule looks for any keywords in the "Low Confidentiality" dictionary.

**Table 31-44** Low Confidentiality Indicators detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword	Low Confidentiality Indicators (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "(confidentiality, low)", "(confidentiality,low)"</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 [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## Password Files policy template

The Password Files policy detects password file formats, such as SAM, password, and shadow.

DCM Rule	<b>Password Filenames</b> This rule looks for the file names "passwd" or "shadow."
DCM Rule	<b>/etc/passwd Format</b> This rule looks for a regular expression pattern with the /etc/passwd format.
DCM Rule	<b>/etc/shadow Format</b> This rule looks for a regular expression pattern with the /etc/shadow format.
DCM Rule	<b>SAM Passwords</b> This rule looks for a regular expression pattern with the SAM format.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

# 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 31-45** Credit Card Numbers, Exact detection rule

Method	Condition	Configuration
Simple rule	Content Matches Exact Data (EDM)	This rule detects credit card numbers. See <a href="#">"Choosing an Exact Data Profile"</a> on page 333.

The Credit Card Numbers, All detection rule detects credit card numbers using the Credit Card Number system Data Identifier.

**Table 31-46** Credit Card Numbers, All detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	Credit Card Numbers, All (Data Identifiers): <ul style="list-style-type: none"> <li>■ Data Identifier: Credit Card Number (narrow) See <a href="#">"Credit Card Number system data identifier"</a> on page 546.</li> <li>■ Severity: High.</li> <li>■ Count all matches.</li> <li>■ Look in envelope, subject, body, attachments.</li> </ul>

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.

**Table 31-47** Magnetic Stripe Data for Credit Cards detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	Magnetic Stripe Data for Credit Cards (Data Identifiers): <ul style="list-style-type: none"><li>■ Data Identifier: Credit Card Magnetic Stripe (medium) See “<a href="#">Credit Card Number system data identifier</a>” on page 546.</li><li>■ Data Severity: High.</li><li>■ Count all matches.</li><li>■ Look in envelope, subject, body, attachments.</li></ul>

See “[Configuring policies](#)” on page 338.

See “[Exporting policy detection as a template](#)” on page 362.

## 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 31-48** PIPEDA detection rule

Detection method type	Description	Excluded combinations
EDM Rule	<p>The PIPEDA detection rule matches any two of the following data items:</p> <ul style="list-style-type: none"> <li>■ Last name</li> <li>■ Bank card</li> <li>■ Medical account number</li> <li>■ Medical record</li> <li>■ Agency number</li> <li>■ Account number</li> <li>■ PIN</li> <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> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>	<p>However, the following combinations do not create a match:</p> <ul style="list-style-type: none"> <li>■ Last name, email</li> <li>■ Last name, phone</li> <li>■ Last name, account number</li> <li>■ Last name, user name</li> </ul>

The PIPEDA Contact Info detection rule looks for a match of two data items, with certain data combinations excepted from matching.

**Table 31-49** PIPEDA Contact Info detection rule

Detection method type	Description
EDM Rule	<p>This rule looks for any two of the following data columns:</p> <ul style="list-style-type: none"> <li>■ Last name</li> <li>■ Phone</li> <li>■ Account number</li> <li>■ User name</li> <li>■ Email</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

**Table 31-50** Canadian Social Insurance Numbers detection rule

Detection method type	Description
DCM Rule	This rule implements the narrow breadth edition of the Canadian Social Insurance Number data identifier.  See <a href="#">“Canadian Social Insurance Number narrow breadth”</a> on page 542.

**Table 31-51** ABA Routing Numbers detection rule

Detection method type	Description
DCM Rule	This rule implements the narrow breadth edition of the ABA Routing Number data identifier.  See <a href="#">“ABA Routing Number narrow breadth”</a> on page 538.

**Table 31-52** Credit Card Numbers, All detection rule

Detection method type	Description
DCM Rule	This rule implements the narrow breadth edition of the Credit Card Number data identifier.  See <a href="#">“Credit Card Number narrow breadth”</a> on page 549.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## Price Information policy template

The Price Information policy detects specific SKU and pricing information at risk of exposure.

<b>EDM Rule</b>	<b>Price Information</b>
	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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Exact Data Matching”](#) on page 368.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

## 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
- vrmf

## DCM Rule

**Media Files Extensions**

This rule looks for file name extensions from the "Media Files Extensions" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

## 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

**Publishing Documents**

This rule looks for the specified file types:

- qexpress
- frame
- aldus\_pagemaker
- 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

# 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

# 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Exact Data Matching”](#) on page 368.

# 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 31-53** Sarbanes-Oxley Documents, Indexed detection rule

Method	Condition	Configuration
Simple rule	Content Matches Indexed Document Profile	See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.

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 31-54** SEC Fair Disclosure Regulation detection rule

Method	Condition	Cofiguration
Compound rule	Content Matches Keyword	<p>SEC Fair Disclosure Regulation (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Match keyword: <b>earnings per share, forward guidance</b></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>■ Match on same component.</li> </ul> <p>The keyword must be in the attachment or file type detected by that condition.</p>
	Message Attachment or File Type Match	<p>SEC Fair Disclosure Regulation (Attachment/File Type):</p> <ul style="list-style-type: none"> <li>■ File type detected: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, and pdf.</li> <li>■ Severity: High.</li> <li>■ Match on: Attachments and same component.</li> </ul>
	Content Matches Keyword	<p>SEC Fair Disclosure Regulation (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Match "[company name]"</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>■ Match on same component.</li> </ul> <p>The keyword must be in the attachment or file type detected by that condition.</p>

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.

**Table 31-55** Financial Information detection rule

Method	Condition	Cofiguration
Compound rule	Content Matches Indexed Document Profile	<b>Financial Information (Attachment/File Type):</b> <ul style="list-style-type: none"> <li>■ Match file type: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, Lotus 1-2-3</li> <li>■ Severity: High.</li> <li>■ Match on attachments, same component.</li> </ul>
	Content Matches Keyword	<b>Financial Information (Keyword Match):</b> <ul style="list-style-type: none"> <li>■ Match "accounts receivable turnover", "adjusted gross margin", "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 (same component).</li> </ul>
	Content Matches Keyword	<b>Financial Information (Keyword Match):</b> <ul style="list-style-type: none"> <li>■ Match "confidential", "internal use only", "proprietary".</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 (same component).</li> </ul>

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-56** 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): <ul style="list-style-type: none"> <li>■ Detect documents from the selected Indexed Document Profile. See <a href="#">“Choosing an Indexed Document Profile”</a> on page 334.</li> <li>■ Match documents with at least 80% content match.</li> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in body, attachments.</li> </ul>

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, Wordperferct, 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 31-57** SEC Fair Disclosure Regulation detection rule

Method	Condition	Configuration
Compound rule	Content Matches Keyword (DCM)	SEC Fair Disclosure Regulation (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "earnings per share", "forward guidance".</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>
	Message Attachment or File Type Match (DCM)	SEC Fair Disclosure Regulation (Attachment/File Type): <ul style="list-style-type: none"> <li>■ Match file type: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, pdf</li> <li>■ Severity: High.</li> <li>■ Match on attachments.</li> <li>■ Require content match to be in the same component (attachment).</li> </ul>
	Content Matches Keyword (DCM)	SEC Fair Disclosure Regulation (Keyword Match): <ul style="list-style-type: none"> <li>■ Match "[company name]" (user defined)</li> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments, same component.</li> <li>■ Case insensitive.</li> <li>■ Match on whole words only.</li> </ul>

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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	<b>Sexually Explicit Keywords, Suspected</b> This rule looks for any three instances of keywords in the "Sex. Explicit Words, Suspect" dictionary.
DCM Rule	<b>Sexually Explicit Keywords, Possible</b> This rule looks for any three instances of keywords in the "Sex. Explicit Words, Possible" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## Source Code policy template

The Source Code policy detects various types of source code at risk of exposure.

IDM Rule	<b>Source Code Documents</b> This rule looks for specific user-provided source code using IDM. This rule returns a match if it detects 80% or more of the source document.
DCM Rule	<b>Source Code Extensions</b> This rule looks for file name extensions from the "Source Code Extensions" dictionary.
DCM Rule	<b>Java Source Code</b> This rule looks for the Java Import Statements or Java Class Files regular expression.
DCM Rule	<b>C Source Code</b> This rule looks for the C Source Code regular expression.
DCM Rule	<b>VB Source Code</b> This rule looks for the VB Source Code regular expression.
DCM Rule	<b>PERL Source Code</b> This rule looks for the three different PERL-related system patterns and regular expressions.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

See [“About implementing Indexed Document Matching”](#) on page 393.

# 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 detects these breaches of confidentiality.

The Email to Affiliates detection exception is evaluated first and applies to email messages sent to affiliates who are legitimately allowed to receive information covered under the State Data Privacy regulations.

**Table 31-58** Email to Affiliates detection exception

Method	Condition(s)	Configuration
Simple exception	Recipient Matches Pattern (DCM)	Email to Affiliates (Recipient): <ul style="list-style-type: none"><li>■ Match e-mail: [affiliate1],[affiliate2]. The "Affiliate Domains" requires editing by the user.</li><li>■ At least 1 recipient(s) must match.</li><li>■ Matches on the entire message.</li></ul>

The State Data Privacy, Consumer Data detection rule looks for an exact match on any three data items, except certain combinations.

**Table 31-59** State Data Privacy, Consumer Data detection rule

Method	Condition	Configuration
Simple rule	Content matches Exact Data (EDM)	<p>This rule looks for a match on any three data items:</p> <ul style="list-style-type: none"> <li>■ First name</li> <li>■ Last name</li> <li>■ Tax payer ID</li> <li>■ Bank card</li> <li>■ Account</li> <li>■ PIN</li> <li>■ State ID</li> <li>■ Drivers license</li> <li>■ Password</li> <li>■ ABA number</li> <li>■ Date of birth</li> </ul> <hr/> <p>However, the following combinations do not match:</p> <ul style="list-style-type: none"> <li>■ First name, last name, pin</li> <li>■ First name, last name, password</li> </ul> <p>See <a href="#">“Choosing an Exact Data Profile”</a> on page 333.</p>

The US Social Security Number Patterns detection rule implements the US SSN narrow breadth system Data Identifier to detect social security numbers.

**Table 31-60** US Social Security Number Patterns detection rule

Detection method	Condition type	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<p>US Social Security Number Patterns:</p> <ul style="list-style-type: none"> <li>■ See <a href="#">“US Social Security Number (SSN) narrow breadth”</a> on page 599.</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 ABA Routing Number data identifier.

**Table 31-61** ABA Routing Numbers detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<p>ABA Routing Numbers:</p> <ul style="list-style-type: none"> <li>■ See <a href="#">“ABA Routing Number narrow breadth”</a> on page 538.</li> <li>■ Severity: High.</li> <li>■ Count all matches.</li> <li>■ Look in envelope, subject, body, attachments.</li> </ul>

The Credit Card Numbers, All detection rule looks for a word from the "Credit Card Number Keywords" dictionary and the credit card number system pattern.

**Table 31-62** Credit Card Numbers, All detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	<p>Credit Card Numbers, All (Data Identifiers):</p> <ul style="list-style-type: none"> <li>■ Credit Card Number See <a href="#">“Credit Card Number narrow breadth”</a> on page 549.</li> <li>■ Severity: High.</li> <li>■ Count all matches.</li> <li>■ Look in envelope, subject, body, attachments</li> </ul>

The CA Drivers License Numbers detection 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.

**Table 31-63** CA Drivers License Numbers detection rule

Detection method	Condition type	Configuration
Simple rule	Content Matches Data Identifier (DCM)	See <a href="#">“Drivers License Number – CA State system data identifier”</a> on page 554.

The NY Drivers License Numbers detection 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.

**Table 31-64** NY Drivers License Numbers detection rule

Detection method	Condition type	Configuration
Simple rule	Content Matches Data Identifier (DCM)	See <a href="#">“Drivers License Number - NY State system data identifier”</a> on page 560.

The FL, MI, and MN Drivers License Numbers detection 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).

**Table 31-65** FL, MI, and MN Drivers License Numbers detection rule

Method	Condition	Configuration
Simple rule	Content Matches Data Identifier (DCM)	See <a href="#">“Drivers License Number - FL, MI, MN States system data identifier”</a> on page 556.

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.

**Table 31-66** IL Drivers License Numbers detection rule

Detection method	Condition type	Configuration
Simple rule	Content Matches Data Identifier (DCM)	See <a href="#">“Drivers License Number - IL State system data identifier”</a> on page 557.

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.

**Table 31-67** NJ Drivers License Numbers detection rule

Detection method	Condition type	Configuration
Simple rule	Content Matches Data Identifier (DCM)	This condition implements the Driver's License Number- NJ State medium breadth system Data Identifier.  See <a href="#">“Drivers License Number- NJ State medium breadth”</a> on page 560.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 regex and a keyword from the "SWIFT Code Keywords" dictionary.

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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	<b>Symantec DLP Awareness</b>  Checks for a keyword match from the "Symantec DLP Awareness" dictionary.
DCM Rule	<b>Symantec DLP Avoidance</b>  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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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	<b>UK Drivers License Numbers</b>  This rule is a compound rule with the following conditions: <ul style="list-style-type: none"><li>■ A single keyword from the "UK Keywords" dictionary</li><li>■ The pattern matching that of the UK drivers license data identifier</li><li>■ Different combinations of the phrase "drivers license" using a data identifier</li></ul>
----------	--

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 regex for UK Passport Numbers (New Type).

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## 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 338.

See ["Exporting policy detection as a template"](#) on page 362.

## 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 31-68** Top Secret Information detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "TOP SECRET//" <ul style="list-style-type: none"> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole or partial words.</li> </ul>

This rule looks for a keyword match on the phrase "SECRET."

**Table 31-69** Secret Information detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "SECRET//" <ul style="list-style-type: none"> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole or partial words.</li> </ul>

This rule looks for a keyword match on the phrases "CLASSIFIED" or "RESTRICTED."

**Table 31-70** Classified or Restricted Information (Keyword Match) detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Match "CLASSIFIED//, //RESTRICTED//" <ul style="list-style-type: none"> <li>■ Severity: High.</li> <li>■ Check for existence.</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Case sensitive.</li> <li>■ Match on whole or partial words.</li> </ul>

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## US Social Security Numbers policy template

The US Social Security Numbers policy detects patterns indicating social security numbers at risk of exposure.

DCM Rule **US Social Security Number Patterns**

This rule looks for a match to the social security number regular expression and a keyword from the dictionary "US SSN Keywords."

See ["Configuring policies"](#) on page 338.

See ["Exporting policy detection as a template"](#) on page 362.

## Violence and Weapons policy template

The Violence and Weapons policy detects violent language and discussions about weapons.

DCM Rule **Violence and Weapons**

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 338.

See ["Exporting policy detection as a template"](#) on page 362.

## Webmail policy template

The Webmail policy detects the use of a variety of Webmail services, including Yahoo, Google, and Hotmail.

Table 31-71

Name	Type	Condition(s)	Description
Yahoo	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL domain <b>mail.yahoo.com</b> .
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>ym/compose</b> .

**Table 31-71** (continued)

Name	Type	Condition(s)	Description
Hotmail	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL domain <b>hotmail.msn.com</b> .
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>compose?&amp;curmbox</b> .
Go	Compound detection rule	Recipient Matches Pattern (DCM)	This condition checks for the URL <b>gmailus.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 <b>aol.com</b> .
		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 <b>gmail.google.com</b> .
		Content Matches Keyword (DCM)	This condition checks for the keyword <b>gmail</b> .

See [“Configuring policies”](#) on page 338.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-72](#) describes its configuration details.

**Table 31-72** Yahoo Message Board detection rule

Method	Condition	Configuration
Compound rule	Content Matches Keyword (DCM)	Yahoo Message Board (Keyword Match): <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match Keyword: <b>post.messages.yahoo.com/bbs</b>.</li> <li>■ Match on whole words only.</li> <li>■ Check for existence (do not count multiple matches).</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Match must occur in the same component for both conditions.</li> </ul>
	AND	
	Content Matches Keyword (DCM)	Yahoo Message Board (Keyword Match): <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match Keyword: board=&lt;<b>enter board number</b>&gt;.</li> <li>■ Match on whole words only.</li> <li>■ Check for existence (do not count multiple matches).</li> <li>■ Look in envelope, subject, body, attachments.</li> <li>■ Match must occur in the same component for both conditions.</li> </ul>

The Finance Message Board URL detection rule detects messages posted to the Yahoo Finance message board.

[Table 31-73](#) describes its configuration.

**Table 31-73** Finance Message Board URL detection rule

Method	Condition	Configuration
Simple rule	Content Matches Keyword (DCM)	Finance Message Board URL (Keyword Match): <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match Keyword: <b>messages.finance.yahoo.com</b>.</li> <li>■ Match on whole words only.</li> <li>■ Check for existence (do not count multiple matches).</li> <li>■ Look in envelope, subject, body, attachments.</li> </ul>

The Board URLs detection rule detects messages posted to the Yahoo or Yahoo Finance message boards by the URL of either.

[Table 31-74](#) describes its configuration details.

**Table 31-74** Board URLs detection rule

Method	Condition	Configuration
Simple rule	Recipient Matches Pattern (DCM)	Board URLs (Recipient): <ul style="list-style-type: none"> <li>■ Recipient URL: <b>messages.yahoo.com,messages.finance.yahoo.com.</b></li> <li>■ At least 1 recipient(s) must match.</li> <li>■ Matches on the entire message (not configurable).</li> </ul>

See [“Creating a policy from a template”](#) on page 321.

See [“Exporting policy detection as a template”](#) on page 362.

## 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 31-75** Yahoo IM detection rule

Method	Condition	Configuration
Compound rule	Content Matches Keyword (DCM)	<p>Yahoo IM (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match keyword: <b>ymsg</b>.</li> <li>■ Match on whole words only.</li> <li>■ Count all matches and report an incident for each match.</li> <li>■ Look for matches in the envelope, subject, body, and attachments.</li> <li>■ Match must occur in the same component for both conditions in the rule.</li> </ul>
	AND	
	Content Matches Keyword (DCM)	<p>Yahoo IM (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match keyword: <b>shttp.msg.yahoo.com</b>.</li> <li>■ Match on whole words only.</li> <li>■ Count all matches and report an incident for each match.</li> <li>■ Look for matches in the envelope, subject, body, and attachments.</li> <li>■ Match must occur in the same component for both conditions in the rule.</li> </ul>

The MSN IM detection rule looks for matches on three keywords in the same message component.

**Table 31-76** MSN IM detection rule

Method	Condition	Configuration
Compound rule	Content Matches Keyword (DCM)	<p>MSN IM (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match keyword: <b>msg</b>.</li> <li>■ Match on whole words only.</li> <li>■ Count all matches and report an incident for each match.</li> <li>■ Look for matches in the envelope, subject, body, and attachments.</li> <li>■ Match must occur in the same component for all conditions in the rule.</li> </ul>
	AND	
	Content Matches Keyword (DCM)	<p>MSN IM (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match keyword: <b>x-msn</b>.</li> <li>■ Match on whole words only.</li> <li>■ Count all matches and report an incident for each match.</li> <li>■ Look for matches in the envelope, subject, body, and attachments.</li> <li>■ Match must occur in the same component for all conditions in the rule.</li> </ul>
	AND	
	Content Matches Keyword (DCM)	<p>MSN IM (Keyword Match):</p> <ul style="list-style-type: none"> <li>■ Case insensitive.</li> <li>■ Match keyword: <b>charset=utf-8</b>.</li> <li>■ Match on whole words only.</li> <li>■ Count all matches and report an incident for each match.</li> <li>■ Look for matches in the envelope, subject, body, and attachments.</li> <li>■ Match must occur in the same component for all conditions in the rule.</li> </ul>

See [“Creating a policy from a template”](#) on page 321.

See [“Exporting policy detection as a template”](#) on page 362.

# Configuring policy response

- [Chapter 32. Responding to policy violations](#)
- [Chapter 33. Configuring and managing response rules](#)
- [Chapter 34. Response rule conditions](#)
- [Chapter 35. 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 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 policy 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 680.

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 policy response rules”](#) on page 691.

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 685.

You can implement conditions to control how and when response rules execute.

See [“About response rule conditions”](#) on page 687.

You can sequence the order of execution for response rules of the same type.

See [“About response rule action execution priority”](#) on page 688.

You must have response rule authoring privileges to create and manage response rules.

See [“About response rule authoring privileges”](#) on page 690.

## 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 policy response rules”](#) on page 691.

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 687.

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 32-1** Response rules by server type

Server type	Description
All detection servers	See <a href="#">“Response rules for all detection servers”</a> on page 681.
Endpoint detection servers	See <a href="#">“Response rules for Endpoint detection”</a> on page 682.
Network detection servers	See <a href="#">“Response rules for Network detection”</a> on page 683.
Classification detection server	See <a href="#">“Response rule for the Classification Server”</a> on page 684.

## Response rules for all detection servers

Symantec Data Loss Prevention provides several response rule actions for Endpoint Prevent, Endpoint Discover, Network Prevent (Web), Network Prevent (Email), and Network Protect.

**Table 32-2** Available response rules for all detection servers

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 <a href="#">“Configuring the Add Note action”</a> on page 714.
Limit Incident Data Retention	Discard or retain matched data with the incident record.  See <a href="#">“Configuring the Limit Incident Data Retention action”</a> on page 714.
Log to a Syslog Server	Log the incident to a syslog server.  See <a href="#">“Configuring the Log to a Syslog Server action”</a> on page 717.
Send Email Notification	Send an email you compose to recipients you specify.  See <a href="#">“Configuring the Send Email Notification action”</a> on page 718.

**Table 32-2** Available response rules for all detection servers (*continued*)

Response rule	Description
Set Attribute	Add a custom value to the incident record. See <a href="#">“Configuring the Set Attribute action”</a> on page 720.
Set Status	Change the incident status to the specified value. See <a href="#">“Configuring the Set Status action”</a> on page 721.

See [“About response rules”](#) on page 680.

See [“Implementing policy response rules”](#) on page 691.

## Response rules for Endpoint detection

Symantec Data Loss Prevention provides several response rule actions for Endpoint Prevent and Endpoint Discover.

**Table 32-3** Available Endpoint response rules

Response rule	Description
Endpoint: FlexResponse	Take custom action using the FlexResponse API. See <a href="#">“Configuring the Endpoint: FlexResponse action”</a> on page 721.
Endpoint Discover: Quarantine File	Quarantine a discovered sensitive file. See <a href="#">“Configuring the Endpoint Discover: Quarantine File action”</a> on page 722.
Endpoint Prevent: Block	Block the transfer of data that violates the policy. For example, block the copy of confidential data from an endpoint computer to a USB flash drive. See <a href="#">“Configuring the Endpoint Prevent: Block action”</a> on page 725.
Endpoint Prevent: Notify	Display an on-screen notification to the endpoint user when confidential data is transferred. See <a href="#">“Configuring the Endpoint Prevent: Notify action”</a> on page 728.

**Table 32-3** Available Endpoint response rules (*continued*)

Response rule	Description
Endpoint Prevent: User Cancel	<p>Allow the user to cancel the transfer of a confidential file. The override is time sensitive.</p> <p>See <a href="#">“Configuring the Endpoint Prevent: User Cancel action”</a> on page 731.</p>

See [“About response rules”](#) on page 680.

See [“Implementing policy response rules”](#) on page 691.

## Response rules for Network detection

Symantec Data Loss Prevention provides several response rule actions for Network Prevent (Web), Network Prevent (Email), and Network Protect (Discover).

**Table 32-4** Available Network response rules

Response rule	Description
Network Prevent: Block FTP Request	<p>Block FTP transmissions.</p> <p>See <a href="#">“Configuring the Network Prevent: Block FTP Request action”</a> on page 734.</p> <p><b>Note:</b> Only available with Network Prevent (Web).</p>
Network Prevent: Block HTTP/S	<p>Block Web postings.</p> <p>See <a href="#">“Configuring the Network Prevent: Block HTTP/S action”</a> on page 734.</p> <p><b>Note:</b> Only available with Network Prevent (Web).</p>
Network Prevent: Block SMTP Message	<p>Block email that causes an incident.</p> <p>See <a href="#">“Configuring the Network Prevent: Block SMTP Message action”</a> on page 736.</p> <p><b>Note:</b> Only available with Network Prevent (Email).</p>

**Table 32-4** Available Network response rules (*continued*)

Response rule	Description
Network Prevent: Modify SMTP Message	<p>Modify sensitive email messages.</p> <p>For example, change the email subject to include information about the violation.</p> <p>See <a href="#">“Configuring the Network Prevent: Modify SMTP Message action”</a> on page 737.</p> <p><b>Note:</b> Only available with Network Prevent (Email).</p>
Network Prevent: Remove HTTP/S Content	<p>Remove confidential content from Web posts.</p> <p>See <a href="#">“Configuring the Network Prevent: Remove HTTP/S Content action”</a> on page 738.</p> <p><b>Note:</b> Only available with Network Prevent (Web).</p>
Network Protect: Copy File	<p>Copy sensitive files to a location you specify.</p> <p>See <a href="#">“Configuring the Network Protect: Copy File action”</a> on page 740.</p> <p><b>Note:</b> Only available with Network Protect.</p>
Network Protect: Quarantine File	<p>Quarantine sensitive files.</p> <p>See <a href="#">“Configuring the Network Protect: Quarantine File action”</a> on page 740.</p> <p><b>Note:</b> Only available with Network Protect.</p>

See [“About response rules”](#) on page 680.

See [“Implementing policy response rules”](#) on page 691.

## 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 32-5** Available Classification response rule

Response rule	Description
Classification: Classify Enterprise Vault Content	<p>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.</p> <p>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.</p>

See [“About response rules”](#) on page 680.

See [“Implementing policy response rules”](#) on page 691.

## 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 rule on demand from the Enforce Server administration console.

See [“About recommended roles for your organization”](#) on page 79.

**Table 32-6** Response rule types

Response rule execution type	Description
Automated Response Rules	<p>When a policy violation occurs, the detection server automatically executes response rule actions.</p> <p>See <a href="#">“About Automated response rules”</a> on page 686.</p>

**Table 32-6** Response rule types (*continued*)

Response rule execution type	Description
Smart Response Rules	When a policy violation occurs, an authorized user manually triggers the response rule.  See <a href="#">“About Smart response rules”</a> on page 686.

See [“About response rule actions”](#) on page 680.

See [“Implementing policy response rules”](#) on page 691.

## 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 687.

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 policy response rules”](#) on page 691.

## 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 680.

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 698.

Only some response rules are available for manual execution.

**Table 32-7** 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 <a href="#">“Configuring the Add Note action”</a> on page 714.
Endpoint: FlexResponse	Take custom action using the FlexResponse plugin API. See <a href="#">“Configuring the Endpoint: FlexResponse action”</a> on page 721.
Log to a Syslog Server	Log the incident to a syslog server for workflow remediation. See <a href="#">“Configuring the Log to a Syslog Server action”</a> on page 717.
Send Email Notification	Send an email you compose to recipients you specify. See <a href="#">“Configuring the Send Email Notification action”</a> on page 718.
Set Status	Set the incident status to the specified value. See <a href="#">“Configuring the Set Status action”</a> on page 721.

See [“Implementing policy response rules”](#) on page 691.

## 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 policy response rules”](#) on page 691.

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 698.

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 697.

**Table 32-8** Available response rule conditions

Condition type	Description
Endpoint Location	Triggers a response action when the endpoint is on or off the corporate network.  See <a href="#">“Configuring the Endpoint Location response condition”</a> on page 703.
Endpoint Device	Triggers a response action when an event occurs on a configured endpoint device.  See <a href="#">“Configuring the Endpoint Device response condition”</a> on page 704.
Incident Type	Triggers a response action when the specified type of detection server reports a match.  See <a href="#">“Configuring the Incident Type response condition”</a> on page 705.
Incident Match Count	Triggers a response action when the volume of policy violations exceeds a threshold or range.  See <a href="#">“Configuring the Incident Match Count response condition”</a> on page 707.
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 <a href="#">“Configuring the Protocol or Endpoint Monitoring response condition”</a> on page 708.
Severity	Triggers a response action when the policy violation is a certain severity level.  See <a href="#">“Configuring the Severity response condition”</a> on page 711.

## About response rule action execution priority

A detection 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 detection server executes two or more different response rules for the same policy, the stronger 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 it.  
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 701.

**Table 32-9** System-defined response rule execution priority

Execution priority (from highest to lowest)	Description
Endpoint Prevent: Block	See <a href="#">“Configuring the Endpoint Prevent: Block action”</a> on page 725.
Endpoint Prevent: User Cancel	See <a href="#">“Configuring the Endpoint Prevent: User Cancel action”</a> on page 731.
Endpoint: FlexResponse	See <a href="#">“Configuring the Endpoint: FlexResponse action”</a> on page 721.
Endpoint Prevent: Notify	See <a href="#">“Configuring the Endpoint Prevent: Notify action”</a> on page 728.
Endpoint Discover: Quarantine File	See <a href="#">“Configuring the Endpoint Discover: Quarantine File action”</a> on page 722.
Limit Incident Data Retention	See <a href="#">“Configuring the Limit Incident Data Retention action”</a> on page 714.
Network Prevent: Block SMTP Message	See <a href="#">“Configuring the Network Prevent: Block SMTP Message action”</a> on page 736.
Network Prevent: Modify SMTP Message	See <a href="#">“Configuring the Network Prevent: Modify SMTP Message action”</a> on page 737.

**Table 32-9** System-defined response rule execution priority (*continued*)

Execution priority (from highest to lowest)	Description
Network Prevent: Remove HTTP/HTTPS Content	See <a href="#">“Configuring the Network Prevent: Remove HTTP/S Content action”</a> on page 738.
Network Prevent: Block HTTP/HTTPS	See <a href="#">“Configuring the Network Prevent: Block HTTP/S action”</a> on page 734.
Network Prevent: Block FTP Request	See <a href="#">“Configuring the Network Prevent: Block FTP Request action”</a> on page 734.
Network Protect: Quarantine File	See <a href="#">“Configuring the Network Protect: Quarantine File action”</a> on page 740.
Network Protect: Copy File	See <a href="#">“Configuring the Network Protect: Copy File action”</a> on page 740.
Classify Content	
Set Status	See <a href="#">“Configuring the Set Status action”</a> on page 721.
Set Attribute	See <a href="#">“Configuring the Set Attribute action”</a> on page 720.
Add Note	See <a href="#">“Configuring the Add Note action”</a> on page 714.
Log to a Syslog Server	See <a href="#">“Configuring the Log to a Syslog Server action”</a> on page 717.
Send Email Notification	See <a href="#">“Configuring the Send Email Notification action”</a> on page 718.

See [“Implementing policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

## 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 [“About policy authoring privileges”](#) on page 313.

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 79.

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 77.

## Implementing policy response rules

You define response rules independent of policies.

See [“About response rules”](#) on page 680.

You must have response rule authoring privileges to create and manage response rules.

See [“About response rule authoring privileges”](#) on page 690.

**Table 32-10** Workflow for implementing policy response rules

Step	Action	Description
Step 1	Review the available response rules.	The <b>Manage &gt; Policies &gt; Response Rules</b> screen displays all configured response rules. See <a href="#">“Manage response rules”</a> on page 695.  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 <a href="#">“About solution packs”</a> on page 311.
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 <a href="#">“About response rule execution types”</a> on page 685.
Step 3	Determine the type of actions you want to implement and any triggering conditions.	See <a href="#">“About response rule conditions”</a> on page 687.  See <a href="#">“About response rule actions”</a> on page 680.
Step 4	Understand the order of precedence among response rule actions of different and the same types.	See <a href="#">“About response rule action execution priority”</a> on page 688.  See <a href="#">“Modifying response rule ordering”</a> on page 701.

**Table 32-10** Workflow for implementing policy response rules (*continued*)

Step	Action	Description
Step 5	Integrate the Enforce Server with an external system (if required for the response rule).	Some response rules may require integration with external systems. These may include: <ul style="list-style-type: none"> <li>■ A SIEM system for the Log to a Syslog Server response rule.</li> <li>■ An SMTP email server for the Send Email Notification response rule</li> <li>■ A Web proxy host for Network Prevent (Web) response rules.</li> <li>■ An MTA for Network Prevent (Email) response rules.</li> </ul>
Step 6	Add a new response rule.	See <a href="#">“Adding a new response rule”</a> on page 697.
Step 7	Configure response rules.	See <a href="#">“Configuring response rules”</a> on page 697.
Step 8	Configure one or more response rule conditions (optional).	See <a href="#">“Configuring response rule conditions”</a> on page 698.
Step 9	Configure one or more response rule actions (required).	You must define at least one action for a valid response rule. See <a href="#">“Configuring response rule actions”</a> on page 699. The action executes when a policy violation is reported or when a response rule condition is matched. See <a href="#">“Response rule best practices”</a> on page 692.
Step 10	Add response rules to policies.	You must have policy authoring privileges to add response rules to policies. See <a href="#">“Adding a response rule to a policy”</a> on page 363.

## 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.

See [“About policy detection development”](#) on page 301.

- Response rules require at least 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 680.
- 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 [“Introduction to detection rules”](#) on page 288.
- 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 338.
- 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 357.
- 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 688.
- Use Smart response rules only where it is appropriate for human intervention.  
See [“About configuring Smart response rules”](#) on page 698.



# 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 680.

You must have response rule authoring privileges to manage and add response rules.

See [“About response rule authoring privileges”](#) on page 690.

**Table 33-1** Response Rules screen actions

Action	Description
Add Response Rule	Click <b>Add Response Rule</b> to define a new response rule. See <a href="#">“Adding a new response rule”</a> on page 697.
Modify Response Rule Order	Click <b>Modify Response Rule Order</b> to modify the response rule order of precedence. See <a href="#">“Modifying response rule ordering”</a> on page 701.
Edit an existing response rule	Click the response rule to modify it. See <a href="#">“Configuring response rules”</a> on page 697.
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 <a href="#">“About removing response rules”</a> on page 702.
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 33-2** Response Rules screen display

Display column	Description
Order	The <b>Order</b> of precedence when more than one response rule is configured. See <a href="#">“Modifying response rule ordering”</a> on page 701.
Rule	The <b>Name</b> of the response rule. See <a href="#">“Configuring response rules”</a> on page 697.
Actions	The type of <b>Action</b> the response rule can take to respond to an incident (required). See <a href="#">“Configuring response rule actions”</a> on page 699.
Conditions	The <b>Condition</b> that triggers the response rule (if any). See <a href="#">“Configuring response rule conditions”</a> on page 698.

See [“Implementing policy response rules”](#) on page 691.

## 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 680.

To add a new response rule

- 1 Click **Add Response Rule** at the **Manage > Policies > Response Rules** screen.

See [“Manage response rules”](#) on page 695.

- 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 686.

- **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 686.

- 3 Click **Next** to configure the response rule.

See [“Configuring response rules”](#) on page 697.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## Configuring response rules

You configure response rules at the **Manage > Policies > Response Rules > Configure Response Rule** screen.

See [“About response rules”](#) on page 680.

To configure a response rule

- 1 Add a new response rule, or modify an existing one.

See [“Adding a new response rule”](#) on page 697.

See [“Manage response rules”](#) on page 695.

- 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 698.  
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 698.
  - 4 Select and configure one or more **Actions**. You must define at least one action.  
See [“Configuring response rule actions”](#) on page 699.
  - 5 Click **Save** to save the response rule definition.  
See [“Manage response rules”](#) on page 695.
- See [“Implementing policy response rules”](#) on page 691.  
See [“Response rule best practices”](#) on page 692.

## 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 686.

See [“Implementing policy response rules”](#) on page 691.

## 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 687.

### To configure a response rule condition

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 2 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 687.

- 3 Choose the condition type from the **Conditions** list.

See [Table 32-8](#) on page 688.

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.

- 4 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 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 policy response rules”](#) on page 691.

### To define a response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 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 33-3](#) on page 700.
- 4 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 701.
- 5 Click **Save** to save the response rule.  
 See [“Manage response rules”](#) on page 695.

**Table 33-3** Configure a response rule action

Detection server	Response rule	Description
All	Add Note	See <a href="#">“Configuring the Add Note action”</a> on page 714.
All	Limit Incident Data Retention	See <a href="#">“Configuring the Limit Incident Data Retention action”</a> on page 714.
All	Log to a Syslog Server	See <a href="#">“Configuring the Log to a Syslog Server action”</a> on page 717.
All	Send Email Notification	See <a href="#">“Configuring the Send Email Notification action”</a> on page 718.
All	Set Attribute	See <a href="#">“Configuring the Set Attribute action”</a> on page 720.
All	Set Status	See <a href="#">“Configuring the Set Status action”</a> on page 721.
Classification	Classify Enterprise Vault Content	
Endpoint	FlexResponse	See <a href="#">“Configuring the Endpoint: FlexResponse action”</a> on page 721.
Endpoint Discover	Quarantine File	See <a href="#">“Configuring the Endpoint Discover: Quarantine File action”</a> on page 722.
Endpoint Prevent	Block	See <a href="#">“Configuring the Endpoint Prevent: Block action”</a> on page 725.
Endpoint Prevent	Notify	See <a href="#">“Configuring the Endpoint Prevent: Notify action”</a> on page 728.

**Table 33-3** Configure a response rule action (*continued*)

Detection server	Response rule	Description
Endpoint Prevent	User Cancel	See <a href="#">“Configuring the Endpoint Prevent: User Cancel action”</a> on page 731.
Network Prevent	Block FTP Request	See <a href="#">“Configuring the Network Prevent: Block FTP Request action”</a> on page 734.
Network Prevent	Block HTTP/S	See <a href="#">“Configuring the Network Prevent: Block HTTP/S action”</a> on page 734.
Network Prevent	Block SMTP Message	See <a href="#">“Configuring the Network Prevent: Block SMTP Message action”</a> on page 736.
Network Prevent	Modify SMTP Message	See <a href="#">“Configuring the Network Prevent: Modify SMTP Message action”</a> on page 737.
Network Prevent	Remove HTTP/S Content	See <a href="#">“Configuring the Network Prevent: Remove HTTP/S Content action”</a> on page 738.
Network Protect	Copy File	See <a href="#">“Configuring the Network Protect: Copy File action”</a> on page 740.
Network Protect	Quarantine File	See <a href="#">“Configuring the Network Protect: Quarantine File action”</a> on page 740.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 688.

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

- 1 Navigate to the **Manage > Policies > Response Rules** screen.  
See [“Manage response rules”](#) on page 695.
  - 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.
  - 4 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.
  - 6 Repeat these steps as necessary to achieve the desired results.
- See [“Implementing policy response rules”](#) on page 691.  
See [“Response rule best practices”](#) on page 692.

## About removing response rules

You can delete response rules at the **Manage > Policies > Response Rules** screen.

See [“Manage response rules”](#) on page 695.

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.

See [“Response rule best practices”](#) on page 692.

# 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 687.

---

**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 697.
- 2 Select the **Endpoint Location** condition from the **Conditions** list.  
See [“Configuring response rule conditions”](#) on page 698.
- 3 Select the endpoint location requirements to trigger actions.  
See [Table 34-1](#) on page 704.

**Table 34-1** 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 policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

See [“Response rule best practices”](#) on page 692.

## 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 687.

You configure endpoint devices at the **System > Agents > Endpoint Devices** screen.

See [“About endpoint device detection”](#) on page 492.

---

**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

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Select the **Endpoint Device** condition from the **Conditions** list.  
See [“Configuring response rule conditions”](#) on page 698.
- 3 Select to detect or except specific endpoint devices.  
See [Table 34-2](#) on page 705.

**Table 34-2** 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 policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

See [“Response rule best practices”](#) on page 692.

## 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 687.

**To configure the Incident Type condition**

- 1 Configure a response rule at the **Configure Response Rule** screen.  
 See [“Configuring response rules”](#) on page 697.
- 2 Choose the **Incident Type** condition from the **Conditions** list.  
 See [“Configuring response rule conditions”](#) on page 698.
- 3 Select one or more incident types.  
 Use the `Ctrl` key to select multiple types.  
 See [Table 34-3](#) on page 706.

**Table 34-3** Incident Type condition parameters

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	Triggers a response rule action for any incident that Network Prevent detects.
Is None Of		Does not trigger a response rule action for any incident that Network Prevent detects.

See [“Implementing policy response rules”](#) on page 691.  
 See [“Manage response rules”](#) on page 695.  
 See [“Response rule best practices”](#) on page 692.

# 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 687.

## To configure the Incident Match Count condition

- 1 Configure a response rule at the **Configure Response Rule** screen.  
 See [“Configuring response rules”](#) on page 697.
- 2 Choose the **Incident Match Count** condition from the **Conditions** list.  
 See [“Configuring response rule conditions”](#) on page 698.
- 3 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 34-4](#) on page 707.

**Table 34-4** 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.
Is 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 policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

See [“Response rule best practices”](#) on page 692.

# 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 687.

### 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 697.
- 2 Choose the **Protocol or Endpoint Monitoring** condition from the **Conditions** list.  
 See [“Configuring response rule conditions”](#) on page 698.
- 3 Use the `Ctrl` key to select multiple, or use the `Shift` key to select a range.  
 See [Table 34-5](#) on page 708.

The system lists any additional network protocols that you configure at the **System > Settings > Protocols** screen.

**Table 34-5** 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	Endpoint CD/DVD	Triggers an action if an endpoint CD/DVD has been written to.
Is None Of		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		Does not trigger action if the endpoint clipboard has been copied to.

**Table 34-5** Protocol or Endpoint Destination condition options (*continued*)

Qualifier	Condition	Description
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	Endpoint Local Drive	Triggers an action if sensitive files are discovered on the local drive.
Is None Of		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.
Is Any Of	Endpoint removable storage device	Triggers an action if sensitive data is copied to a removeable storage device.
Is None Of		Does not trigger action if sensitive data is copied to a removeable 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		Does not trigger action if sensitive data is sent through AIM.

**Table 34-5** Protocol or Endpoint Destination condition options (*continued*)

Qualifier	Condition	Description
Is Any Of	IM:MSN	Triggers an action if sensitive data is sent through MSN.
Is None Of		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		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		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		Does not trigger action if sensitive data is sent through SMTP.
Is Any Of	TCP:HTTPS	Triggers an action if sensitive data is sent through TCP:HTTPS.
Is None Of		Does not trigger action if sensitive data is sent through TCP:HTTPS.
Is Any Of	TCP:SSH	Triggers an action if sensitive data is sent through TCP:SSH.
Is None Of		Does not trigger action if sensitive data is sent through TCP:SSH.
Is Any Of	TCP:SSL	Triggers an action if sensitive data is sent through TCP:SSL.
Is None Of		Does not trigger action if sensitive data is sent through TCP:SSL.
Is Any Of	TCP:Telnet	Triggers an action if sensitive data is sent through TCP:Telnet.
Is None Of		Does not trigger action if sensitive data is sent through TCP:Telnet.

See [“Implementing policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

See [“Response rule best practices”](#) on page 692.

## 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 687.

### To configure the Severity condition

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 2 Select the **Severity** condition from the **Conditions** list.

See [“Configuring response rule conditions”](#) on page 698.

- 3 Select one or more severity levels.

Use the `Ctrl` key to select multiple; use the `Shift` key to select a range.

See [Table 34-6](#) on page 711.

**Table 34-6** 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.

**Table 34-6** Severity condition matches (*continued*)

Parameter	Severity	Description
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 policy response rules”](#) on page 691.

See [“Manage response rules”](#) on page 695.

See [“Response rule best practices”](#) on page 692.

# 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 Set Attribute action](#)
- [Configuring the Set Status 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 Prevent: Block FTP Request action](#)
- [Configuring the Network Prevent: Block HTTP/S action](#)
- [Configuring the Network Prevent: Block SMTP Message action](#)
- [Configuring the Network Prevent: Modify SMTP Message action](#)
- [Configuring the Network Prevent: 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 680.

The Add Note response rule action is available for all types of detection servers.

See [“Response rules for all detection servers”](#) on page 681.

### To configure the Add Note action

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 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 699.

- 3 Click **Save** to save the configuration.

See [“Manage response rules”](#) on page 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule is available for all types of detection servers.

See [“Response rules for all detection servers”](#) on page 681.

### To configure incident data retention

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 2 Add the action type **All: Limit Incident Data Retention** from the **Actions** list.

See [“Configuring response rule actions”](#) on page 699.

- 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 715.
- 4 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 716.
- 5 Click **Save** to save the response rule configuration.  
See [“Manage response rules”](#) on page 695.  
See [“Implementing policy response rules”](#) on page 691.  
See [“Response rule best practices”](#) on page 692.

## 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.

See [“Configuring the Limit Incident Data Retention action”](#) on page 714.

**Table 35-1** 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 all 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.

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 714.

---

**Note:** The default data retention behavior for network incidents applies to Network Prevent (Web) and Network Prevent (Email) incidents. The default behavior does not apply to Network Protect (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 35-2** Discarding data from network incidents

Parameter	Description
Discard Original Message	Check this option to discard the original message. Use this configuration to save disk space when you are only interested in statistical data.
Discard Attachment	Select <b>All</b> 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.

# 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 680.

This response rule action is available for all types of detection servers.

See [“Response rules for all detection servers”](#) on page 681.

You must integrate the Enforce Server with the syslog server to implement this response rule action.

See [“Enabling a syslog server”](#) on page 113.

## To configure the Log to a Syslog Server response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

- 2 Add the **Log to a Syslog Server** action type from the **Actions** list.

See [“Configuring response rule actions”](#) on page 699.

- 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.

- 6 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 - Error
- 4 - Warning
- 5 - May need attention
- 6 - Informational
- 7 - Debugging

- 7 **Save** the response rule.

See [“Manage response rules”](#) on page 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule action is available for all types of detection servers.

See [“Response rules for all detection servers”](#) on page 681.

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 115.

### To configure the Send Email Notification response rule action

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **All: Send Email Notification** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 3 Configure the recipient(s), sender, format, incident inclusion, and messages per day.  
See [Table 35-3](#) on page 718.
- 4 Configure the **Notification Content** of the email notification: language, subject, body.  
See [Table 35-4](#) on page 719.
- 5 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.

**Table 35-3** Sender and recipient information

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.

**Table 35-3** Sender and recipient information (*continued*)

Parameter	Description
Custom To	Enter one or more specific email addresses separated by commas.  This option can include any custom attributes designated as email addresses (such as "Manager Email").  See <a href="#">"Configuring custom attributes"</a> on page 799.
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 35-4** Notification content

Parameter	Description
Language	Select the language for the message from the drop-down menu.
Add Language	Click the icon to add multiple language(s) for the message.  See <a href="#">"About Endpoint Prevent response rules in different locales"</a> on page 1077.
Subject	Enter a subject for the message that indicates what the message is about.
Body	Enter the body of the message.

**Table 35-4** Notification content (*continued*)

Parameter	Description
Insert Variables	<p>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.</p> <p>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.</p> <p><b>A message has violated the following rules in \$POLICY\$: \$RULES\$</b></p>

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule action is available for all detection servers.

See [“Response rules for all detection servers”](#) on page 681.

The Set Attribute action is based on custom attributes you define at the **System > Incident Data > Attributes** screen.

See [“About custom attributes”](#) on page 797.

**To configure the Set Attribute action**

- 1 Configure a response rule at the **Configure Response Rule** screen.  
 See [“Configuring response rules”](#) on page 697.
- 2 Add the **All: Set Attribute** action type from the **Actions** list.  
 See [“Configuring response rule actions”](#) on page 699.
- 3 Select the **Attribute** from the drop-down list (if more than one custom attribute is defined).
- 4 Enter an incident status **Value** for the selected custom attribute.
- 5 Click **Save** to save the configuration.  
 See [“Manage response rules”](#) on page 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule is available for all detection servers.

See [“Response rules for all detection servers”](#) on page 681.

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 793.

**To configure the Set Status response rule action**

1 Configure a response rule at the **Configure Response Rule** screen.

See [“Configuring response rules”](#) on page 697.

2 Add the **All: Set Status** action type from the **Actions** list.

3 See [“Configuring response rule actions”](#) on page 699.

4 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

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

See [“Manage response rules”](#) on page 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 1089.

This response rule is available for Endpoint Discover.

See [“Response rules for Endpoint detection”](#) on page 682.

#### To configure the Endpoint: FlexResponse response rule action

- 1 Configure a response rule at the **Configure Resonse Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **Endpoint: FlexResponse** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 3 Enter the FlexResponse plugin **Name** and configure its **Parameters**.  
See [Table 35-5](#) on page 722.
- 4 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.

**Table 35-5** 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 <b>Add Parameter</b> to add one or more parameters to the script. Enter the <b>Key/Value</b> pair for each parameter.
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 <a href="#">“About the credential store”</a> on page 99.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 1070.

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 [“How to implement Endpoint Discover”](#) on page 1067.

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 688.

**To configure the Endpoint Discover: Quarantine File response rule action**

- 1** Configure a response rule at the **Configure Resonse Rule** screen.  
 See [“Configuring response rules”](#) on page 697.
- 2** Add the **Endpoint Discover: Quarantine File** action type from the **Actions** list.  
 See [“Configuring response rule actions”](#) on page 699.
- 3** Enter the **Quarantine Path** and the **Marker File** settings.  
 See [Table 35-6](#) on page 723.
- 4** Click **Save** to save the configuration.  
 See [“Manage response rules”](#) on page 695.

**Table 35-6** Endpoint Discover: Quarantine File response rule action parameters

Parameter	Description
<b>Quarantine Path</b>	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 computer, or can be on a remote file share. EFS folders can also be used as the quarantine location.

**Table 35-6** Endpoint Discover: Quarantine File response rule action parameters  
(continued)

Parameter	Description
<b>Access Mode</b>	<p>If your secure location is on a remote file share, you must select how the Symantec DLP Agent accesses that file share.</p> <p>Select one of the following credential access types:</p> <ul style="list-style-type: none"> <li>■ Anonymous Access</li> <li>■ Use Saved Credentials</li> </ul> <p>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.</p> <p><b>Note:</b> EFS folders cannot accept anonymous users.</p> <p>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:</p> <pre>domain\user</pre> <p>You must enter the specified credentials you want to use through the System Credentials page.</p> <p>See <a href="#">“Configuring endpoint credentials”</a> on page 100.</p>
<b>Marker File</b>	<p>Select the <b>Leave marker in place of the remediated file</b> checkbox to create a placeholder file that replaces the confidential file.</p>
<b>Marker Text</b>	<p>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.</p> <p>To specify the marker text, select the variable from the <b>Insert Variable</b> list.</p> <p>For example, for Marker Text you might enter:</p> <p><b>A message has violated the following rules in \$POLICY\$: \$RULES</b></p> <p>Or, you might enter:</p> <p><b>\$FILE_NAME\$ has been moved to \$QUARANTINE_PARENT_PATH\$</b></p>

See [“About response rule actions”](#) on page 680.

See [“Response rules for Endpoint detection”](#) on page 682.

See [“Response rule best practices”](#) on page 692.

# Configuring the Endpoint Prevent: Block action

The Endpoint Prevent: Block response rule action blocks the movement of confidential data on the endpoint computer and optionally displays an on-screen notification to the endpoint user.

See [“About response rule actions”](#) on page 680.

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 [“How to implement Endpoint Discover”](#) on page 1067.

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 688.

---

**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 Resonse Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **Endpoint Prevent: Block** action type from the **Actions** list.
- 3 See [“Configuring response rule actions”](#) on page 699.
- 4 Enter the **Endpoint Notification Content** settings.  
See [Table 35-7](#) on page 725.
- 5 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.

**Table 35-7** 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 <a href="#">“About Endpoint Prevent response rules in different locales”</a> on page 1077.  See <a href="#">“Setting Endpoint Prevent response rules for different locales”</a> on page 1078.

**Table 35-7** Endpoint Prevent: Block response rule action parameters (*continued*)

Parameter	Configuration
Display Alert Box with this message	<p>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.</p> <p>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.</p> <p>Optionally, you can configure the on-screen notification to include user justifications as well as an option for users to enter their own justification.</p>
Insert Variable	<p>Select the variables to include in the on-screen notification to the endpoint when the system blocks an attempt to copy confidential data.</p> <p>You can select variables based on the following types:</p> <ul style="list-style-type: none"> <li>■ Application</li> <li>■ Content Name</li> <li>■ Content Type</li> <li>■ Device Type</li> <li>■ Policy Names</li> <li>■ Protocol</li> </ul>

**Table 35-7** Endpoint Prevent: Block response rule action parameters (*continued*)

Parameter	Configuration
Allow user to choose explanation	<p>Select this option to display up to four user justifications in the on-screen notification. When the notification appears on the endpoint computer, 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.</p> <p><b>Justification:</b></p> <ul style="list-style-type: none"> <li>■ User Education</li> <li>■ Broken Business Process</li> <li>■ Manager Approved</li> <li>■ False positive</li> </ul> <p>Each justification entry consists of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Check box</b> 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.</li> <li>■ <b>Justification</b> 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.</li> <li>■ <b>Option Presented to End User</b> 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.</li> </ul> <p>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.</p> <p><b>Note:</b> You should be selective when adding new justifications. Deleting new justifications is not currently supported.</p>
Allow user to enter text explanation	<p>Select this option to include a text box into which users can enter their own justification.</p>

See [“Response rules for Endpoint detection”](#) on page 682.

See [“Response rule best practices”](#) on page 692.

# 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 680.

This response rule action is available for Endpoint Prevent.

See [“How to implement Endpoint Prevent”](#) on page 1075.

---

**Note:** The notify action is not triggered for a copy of sensitive data to a local drive.

---

## To configure the Endpoint Prevent: Notify action

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.  
Add the **Endpoint Prevent: Notify** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 2 Configure the action parameters.  
See [Table 35-8](#) on page 728.
- 3 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.

**Table 35-8** Endpoint Prevent: Notify response rule action 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 <a href="#">“About Endpoint Prevent response rules in different locales”</a> on page 1077. See <a href="#">“Setting Endpoint Prevent response rules for different locales”</a> on page 1078.

**Table 35-8** Endpoint Prevent: Notify response rule action parameters  
(continued)

Parameter	Description
Display Alert Box with this message	<p>This field is required for Endpoint Notify actions. Select this option to display an on-screen notification to the endpoint user.</p> <p>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.</p> <p>Optionally, you can configure the on-screen notification to include user justifications as well as the option for users to enter their own justifications.</p>
Insert Variable	<p>Select the variables that you want to include in the on-screen notification to the endpoint user.</p> <p>You can select variables based on the following types:</p> <ul style="list-style-type: none"><li>■ Application</li><li>■ Content Name</li><li>■ Content Type</li><li>■ Device Type</li><li>■ Policy Names</li><li>■ Protocol</li></ul>

**Table 35-8** Endpoint Prevent: Notify response rule action parameters  
*(continued)*

Parameter	Description
Allow user to choose explanation	<p>Select this option to display up to four user justifications in the on-screen notification. When the notification appears on the endpoint computer, 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.</p> <p>Available Justifications:</p> <ul style="list-style-type: none"> <li>■ Broken Business Process</li> <li>■ False positive</li> <li>■ Manager Approved</li> <li>■ User Education</li> <li>■ Custom (new justification)</li> </ul> <p>Each justification entry consists of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Check box</b>                      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.</li> <li>■ <b>Justification</b>                      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.</li> <li>■ <b>Option Presented to End User</b>                      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.</li> </ul> <p>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.</p> <p><b>Note:</b> You should be selective in adding new justifications. Deleting new justifications is not currently supported.</p>
Allow user to enter text explanation	<p>Select this option to include a text box into which users can enter their own justification.</p>

See [“Response rules for Endpoint detection”](#) on page 682.

See [“Response rule best practices”](#) on page 692.

## 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 680.

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 1075.

### To configure the Endpoint Prevent: User Cancel action

- 1 Configure a response rule at the **Configure Response Rule** screen.  
 See [“Configuring response rules”](#) on page 697.  
 Add the **Endpoint Prevent: User Cancel** action type from the **Actions** list.  
 See [“Configuring response rule actions”](#) on page 699.
- 2 Configure the **Endpoint Prevent: User Cancel** parameters.  
 See [Table 35-9](#) on page 731.
- 3 Click **Save** to save the configuration.  
 See [“Manage response rules”](#) on page 695.

**Table 35-9** 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 <a href="#">“About Endpoint Prevent response rules in different locales”</a> on page 1077. See <a href="#">“Setting Endpoint Prevent response rules for different locales”</a> on page 1078.

**Table 35-9** Endpoint Prevent: User Cancel parameters (*continued*)

Parameter	Description
Pre-timeout warning	<p>This field is required to notify users that they have a limited amount of time to respond to the incident.</p> <p>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.</p>
Post-timeout message	<p>This field notifies users that the amount of time to override the policy has expired. The data transfer was blocked.</p> <p>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.</p>
Display Alert Box with this message	<p>This field is required for Endpoint User Cancel actions. Select this option to display an on-screen notification to the endpoint user.</p> <p>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.</p> <p>Optionally, you can configure the on-screen notification to include user justifications as well as the option for users to enter their own justifications.</p>
Insert Variable	<p>Select the variables that you want to include in the on-screen notification to the endpoint user.</p> <p>You can select variables based on the following types:</p> <ul style="list-style-type: none"> <li>■ Application</li> <li>■ Content Name</li> <li>■ Content Type</li> <li>■ Device Type</li> <li>■ Policy Name</li> <li>■ Protocol</li> <li>■ Timeout Counter</li> </ul> <p><b>Note:</b> You must use the Timeout Counter variable to display how much time remains before blocking the data transfer.</p>

**Table 35-9** Endpoint Prevent: User Cancel parameters (*continued*)

Parameter	Description
Allow user to choose explanation.	<p>Select this option to display up to four user justifications in the on-screen notification. When the notification appears on the endpoint computer, 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.</p> <p>Available Justifications:</p> <ul style="list-style-type: none"> <li>■ Broken Business Process</li> <li>■ False positive</li> <li>■ Manager Approved</li> <li>■ User Education</li> <li>■ Custom (new justification)</li> </ul> <p>Each justification entry consists of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Check box</b> 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.</li> <li>■ <b>Justification</b> 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.</li> <li>■ <b>Option Presented to End User</b> 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.</li> </ul> <p>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.</p> <p><b>Note:</b> You should be selective in adding new justifications. Deleting new justifications is not currently supported.</p>
Allow user to enter text explanation.	Select this option to include a text box into which users can enter their own justification.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## Configuring the Network Prevent: Block FTP Request action

The Network Prevent: Block FTP Request response rule action blocks any file transfer by FTP on your network.

See [“About response rule actions”](#) on page 680.

This response rule is only available for Network Prevent (Web) integrated with a proxy server.

See [“Configuring Network Prevent \(Web\) Server”](#) on page 829.

**To configure the Network Prevent: Block FTP Request response rule action**

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **Network Prevent: 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 699.

- 3 Click **Save** to save the configuration.

See [“Manage response rules”](#) on page 695.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## Configuring the Network Prevent: Block HTTP/S action

The Network Prevent: Block HTTP/S response rule action blocks the transmission of Web content that Network Prevent (Web) detects. This action also blocks Web-based email messages and attachments.

See [“About response rule actions”](#) on page 680.

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.

See [“Configuring Network Prevent \(Web\) Server”](#) on page 829.

### To configure the Network Prevent: Block HTTP/S response rule action

- 1 Integrate Network Prevent (Web) with a proxy server.  
See [“Network Prevent \(Web\) Server—basic configuration”](#) on page 159.
- 2 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 3 Add the **Network Prevent: Block HTTP/S** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 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.

---

- 5 Click **Save** to save the configuration of the response rule.

Certain applications may not provide an adequate response to the Network Prevent: 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 Prevent: 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.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

# 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 680.

This response rule action is only available with Network Prevent (Email).

See [“Response rules for Network detection”](#) on page 683.

You must integrate the Network Prevent (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

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **Network Prevent: Block SMTP Message** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 3 Configure the Block SMTP Message action parameters.  
See [Table 35-10](#) on page 736.
- 4 Click **Save** to save the response rule.  
See [“Manage response rules”](#) on page 695.

**Table 35-10** 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.

**Table 35-10** Network Prevent: Block SMTP Message parameters (*continued*)

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.

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule action is only available for Network Prevent (Email).

See [“Response rules for Network detection”](#) on page 683.

### To configure the Network Prevent: Modify SMTP Message action

- 1 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
- 2 Add the **Network Prevent: Modify SMTP Message** action type from the **Actions** list.  
See [“Configuring response rule actions”](#) on page 699.
- 3 Configure the action parameters.  
See [Table 35-11](#) on page 738.
- 4 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.

**Table 35-11** Network Prevent: Modify SMTP Message parameters

Parameter	Description
Subject	<p>Select the type of modification to make to the subject of the message from the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Do not Modify</b> – No text is changed in the subject.</li> <li>■ <b>Prepend</b> – New text is added to the beginning of the subject.</li> <li>■ <b>Append</b> – New text is added to the end of the subject.</li> <li>■ <b>Replace With</b> – New text completely replaces the old subject text.</li> </ul> <p>If the subject text is currently modified, specify the new text.</p> <p>For example, if you want to prepend "VIOLATION" to the subject of the message, select <b>Prepend</b> and enter <b>VIOLATION</b> in the text field.</p>
Headers	Enter a unique name and a value for each header you want to add to the message (up to three).

See [“Implementing policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## Configuring the Network Prevent: Remove HTTP/S Content action

The Network Prevent: 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 response rule action only applies to HTTP/S POST commands; it does not apply to GET commands.

See [“About response rule actions”](#) on page 680.

This response rule action is only available for Network Prevent (Web).

See [“Response rules for Network detection”](#) on page 683.

Symantec Data Loss Prevention recognizes Web form fields for selected Web mail, blog, and social networking sites. If Network Prevent (Web) cannot remove confidential data for a Web site it recognizes, it creates a system event and performs a configured fallback option.

**Note:** Network Prevent (Web) removes content for file uploads and Web mail attachments even for those sites that it does not recognize for HTTP content removal.

**To configure the Network Prevent: Remove HTTP/S Content action**

- 1 Configure a response rule at the **Configure Response Rule** screen.  
 See [“Configuring response rules”](#) on page 697.
- 2 Add the **Network Prevent: Remove HTTP/S Content** action type from the **Actions** list.  
 See [“Configuring response rule actions”](#) on page 699.
- 3 Configure the action parameters.  
 See [Table 35-12](#) on page 739.
- 4 Click **Save** to save the configuration.  
 See [“Manage response rules”](#) on page 695.

**Table 35-12** Network Prevent: Remove HTTP/S Content 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	<p>The action to take if Network Prevent (Web) cannot remove confidential information that was detected in an HTTP or HTTPS post.</p> <p>The available options are <b>Block</b> (the default) and <b>Allow</b>.</p> <p><b>Note:</b> Network Prevent (Web) removes confidential data in file uploads and 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 Network Prevent (Web) detects confidential content in a recognized Web form, but it cannot remove the content.</p>
Rejection Message	The message that Network 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 policy response rules”](#) on page 691.

See [“Response rule best practices”](#) on page 692.

## 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 680.

This response rule action is only available for Network Discover that is configured for Network Protect.

See [“Response rules for Network detection”](#) on page 683.

### To configure the Network Protect: Copy File response rule action

- 1 Configure a network file share and specify a location to copy files to.  
See [“Configuring Network Protect for file shares”](#) on page 906.
  - 2 Configure a response rule at the **Configure Response Rule** screen.  
See [“Configuring response rules”](#) on page 697.
  - 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 699.
  - 4 Click **Save** to save the configuration.  
See [“Manage response rules”](#) on page 695.
- See [“Implementing policy response rules”](#) on page 691.  
See [“Response rule best practices”](#) on page 692.

## Configuring the Network Protect: Quarantine File action

The Network Protect: Quarantine File response rule action quarantines a file that that the detection server identifies as sensitive or protected.

See [“About response rule actions”](#) on page 680.

This response rule action is only available for Network Discover that is configured for Network Protect.

See [“Response rules for Network detection”](#) on page 683.

**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 697.
- 2 Add the **Network Protect: Quarantine File** action type from the **Actions** list.  
 See “[Configuring response rule actions](#)” on page 699.
- 3 Configure the **Network Protect: Quarantine File** parameters.  
 See [Table 35-13](#) on page 741.
- 4 Click **Save** to save the configuration.  
 See “[Manage response rules](#)” on page 695.

**Table 35-13** Network Protect: Quarantine File configuration parameters

Parameter	Description
Marker File	<p>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.</p> <p><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 <b>.txt</b> appended to the end. For example, if the original file name is <code>accounts.pdf</code>, the marker file name is <code>accounts.pdf.txt</code>.</p>
Marker Text	<p>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.</p> <p>To specify marker text, select the variable from the <b>Insert Variable</b> list.</p> <p>For example, for Marker Text you might enter:</p> <p><b>A message has violated the following rules in \$POLICY\$: \$RULES</b></p> <p>Or, you might enter:</p> <p><b>\$FILE_NAME\$ has been moved to \$QUARANTINE_PARENT_PATH\$</b></p>

See “[Implementing policy response rules](#)” on page 691.

See “[Response rule best practices](#)” on page 692.

**Configuring the Network Protect: Quarantine File action**

# Managing data loss incidents

- [Chapter 36. Managing incident reports](#)
- [Chapter 37. Report filters and summary options](#)
- [Chapter 38. About incident remediation](#)
- [Chapter 39. Managing custom attributes and status values for incidents](#)



# Managing incident reports

This chapter includes the following topics:

- [About Symantec Data Loss Prevention reports](#)
- [About strategies for using reports](#)
- [Setting report preferences](#)
- [About dashboard reports and executive summaries](#)
- [About summary reports](#)
- [About custom reports and dashboards](#)

## 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.

Symantec Data Loss Prevention tracks incidents for all detection servers. These servers include Network Discover Server, Network Monitor Server, Network Prevent (Email) Server, Network Prevent (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 747.

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**, or **Discover**.
- 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.
- 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**, 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 753.

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 753.
- The **Network** section contains Symantec-provided incident lists, summaries, and dashboards for network 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.

## 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 quickly 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 748.

See [“About summary reports”](#) on page 751.

- 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 783.

## Setting report preferences

You can specify the reports that Symantec Data Loss Prevention displays in the navigation panel for each of the report types. You can also specify the report that displays in the initial window.

You can specify which reports appear in the navigation panel at the left. You can also specify the report that displays at logon for your current role.

### To set reporting preferences

- 1 In the Enforce Server administration console, on the **Incidents** menu, click **Incident Reports**.
- 2 On the **Incident Reports** screen that appears, click **Edit Preferences**.  
The **Edit Report Preferences** screen lists any saved reports (for all your assigned roles).  
The screen also lists Network, Endpoint, and Discover reports.
- 3 To specify a default report for the current role, locate the **Home Page for current\_role** drop-down list and select a report. Symantec Data Loss Prevention displays this report whenever you first log on under the current role.
- 4 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**.
- 5 After changing your preferences, click **Save**.

See [“About custom reports and dashboards”](#) on page 753.

## 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, and Discover incident reports.

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, 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 753.

To edit the contents of any custom dashboard, go to the desired dashboard and click **Customize** near the top of the screen.

To display a custom dashboard at logon, specify it as the default logon report.

See [“Setting report preferences”](#) on page 747.

## Viewing dashboards

This procedure shows you how to view a dashboard.

### To view a dashboard

- 1 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**.

- 2 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 786.

See [“About summary reports”](#) on page 751.

## 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

- 1 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.
- 6 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 115.

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.

- 7 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.

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.

- 8 Click **Save**.
- 9 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 758.

## 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 reports”](#) on page 777.

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

- 1 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.

- 2 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.
- 4 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 786.

## Creating summary reports

This procedure shows you how to create a summary report.

### To create a summary report from an incident list

- 1 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 reports”](#) on page 777.

- 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 755.

## 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 custom reports for all 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 751.

See [“Summary options for reports”](#) on page 777.

See [“General filters for reports”](#) on page 763.

See [“Advanced filter options for reports”](#) on page 766.

**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 750.

**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 758.

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 755.



Click this icon next to a report to display the screen to 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 755.

- ✘ 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.

## Filtering reports

You can filter an incident list or summary report.

### To filter an incident list

- 1 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.
- 3 Modify the default filters as wanted. For example, from the **Status** filter drop-down lists, select **Equals** and **New**.  
For Network and Endpoint reports, the default filters are **Date** and **Status**.  
For Discover reports, default filters are **Status**, **Scan**, and **Target ID**.
- 4 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 755.

## 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 you choose to share the report, Symantec Data Loss Prevention displays it for any user that is logged on under your role.

See [“About custom reports and dashboards”](#) on page 753.

You can edit the report later on the **Edit Preferences** screen.

See [“Editing custom dashboards and reports”](#) on page 758.

Optionally, you can schedule the report to be run automatically on a regular basis.

See [“Scheduling custom incident reports”](#) on page 756.

#### To save a custom report

- 1 Set up a customized filter or summary report.

See [“About custom reports and dashboards”](#) on page 753.

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.

- 4 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*.

See [“Creating and distributing aggregated incident reports to data owners”](#) on page 788.

**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 115.

**2 Specify the Delivery Details:**

<b>To:</b>	Select whether the report is sent to specified email addresses or to the data owners.
<b>Manual - Sent to specified e-mail addresses</b>	Enter the specific email addresses manually in the text box.
<b>Auto - Send to incident data owners</b>	<p>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.</p> <p>See <a href="#">“Configuring the Enforce Server to send email alerts”</a> on page 115.</p> <p>If you select to have the report sent to the incident data owners, then the email address in the incident attribute <b>Data Owner Email Address</b> is the address where the report is sent.</p> <p>This <b>Data Owner Email Address</b> must be set manually, or with a lookup plug-in.</p> <p>See <a href="#">“Creating and distributing aggregated incident reports to data owners”</a> on page 788.</p> <p>See the <i>Symantec Data Loss Prevention Data Insight Implementation Guide</i>.</p> <p>A maximum of 10000 incidents can be distributed per data owner.</p>
<b>CC:</b>	Enter the email addresses manually in the text box.
<b>Subject:</b>	Use the default subject or modify it.
<b>Body:</b>	<p>Enter the body of the email.</p> <p>Response action variables can also be entered in the body.</p>

- 3 In the **Schedule Delivery** section, specify the delivery schedule.
- 4 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 115.
- 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.
- 6 You can also enter new values for any custom attributes.  

These attributes must be already set up.

See [“About incident status attributes”](#) on page 793.
- 7 Select one of the custom attributes from the drop-down list.
- 8 Click **Add**.
- 9 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**.

## Editing custom dashboards and reports

You can edit any custom report or dashboard that you create.

### To edit a custom dashboard or report

- 1 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.
- 2 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 755.
- 3 When you finish editing, click **Save**.

## Deleting custom dashboards and reports

You can delete any custom report or dashboard that you create.

### To delete a custom dashboard or report

- 1 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.

- 2 Click the delete icon next to the report or dashboard to delete it.
- 3 Click **OK** to confirm.
- 4 Symantec Data Loss Prevention deletes the report, and removes it from the **Incident Reports** screen.



# Report filters and summary options

This chapter includes the following topics:

- [About filters and summary options for reports](#)
- [General filters for reports](#)
- [Advanced filter options for reports](#)
- [Summary options for reports](#)

## About filters and summary options for reports

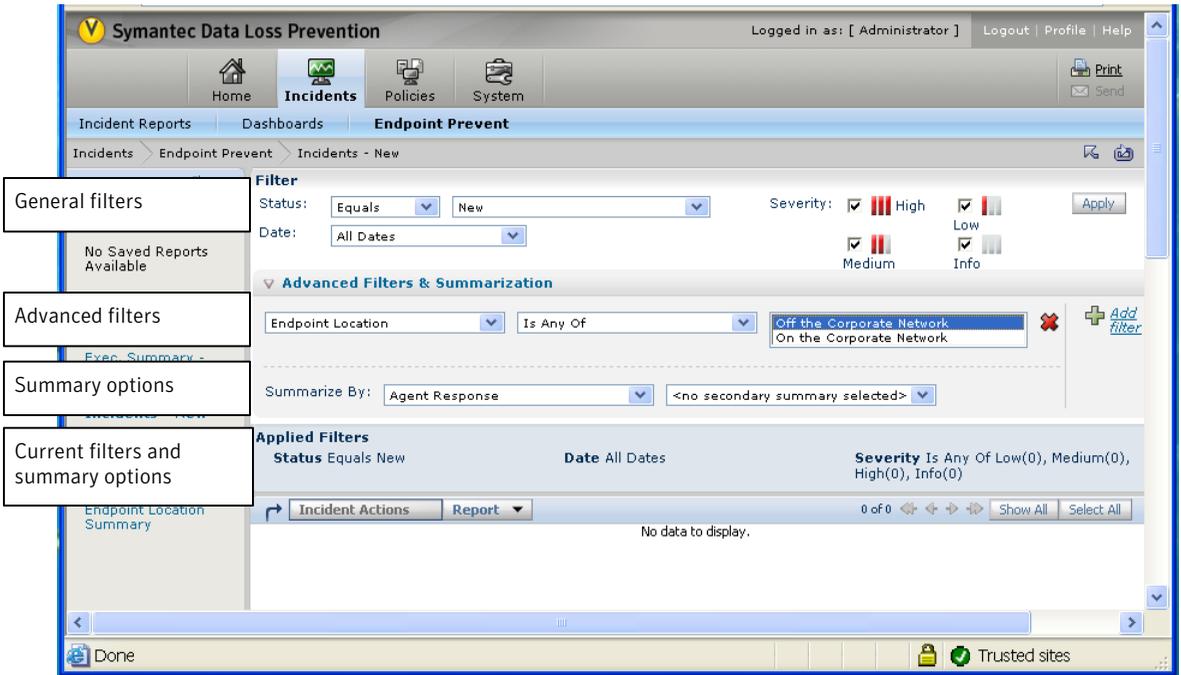
You can set a number of filters and summaries for Symantec Data Loss Prevention incident reports.

These filters let you see the incidents and incident data in different ways.

The set of filters apply separately to Network, Endpoint, and Storage events.

[Figure 37-1](#) shows the locations of the options to filter and summarize reports.

Figure 37-1 Filter and summary options



The filters and summary options are in the following sections:

**General filters**                      The general filter options are the most commonly used. They are always visible in the incident list report. See “[General filters for reports](#)” on page 763.

**Advanced filters**                      The advanced filters provide many additional filter options. You must click the **Advanced Filters & Summarization** bar, and then click **Add Filter** to view these filter options. See “[Advanced filter options for reports](#)” on page 766.

Summary options      The summary options      See “[Summary options for reports](#)” on page 777.

provide ways to summarize the 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 745.

## 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 37-1](#) lists the general filter options for report status values.

You can also create custom status values.

See “[About incident status attributes](#)” on page 793.

These status filters are available for Network, Endpoint, and Discover incidents.

**Table 37-1**      General filters for status values

Name	Description
<b>Equals</b>	The status is equal to the field that is selected in the next drop-down.
<b>Is Any Of</b>	The status can be any of the fields that are selected in the next drop-down. Shift-click to select multiple fields.
<b>Is None Of</b>	The status is none of the fields that are selected in the next drop-down. Shift-click to select multiple fields.

[Table 37-2](#) lists the general filter options by date.

These date filters are available for Network and Endpoint incidents.

**Table 37-2** General filters by date

Name	Description
<b>All Dates</b>	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.
<b>Current Quarter to Date</b>	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.
<b>Current Year to Date</b>	All of the incidents that have been reported for the current year up to today's date.
<b>Custom</b>	A custom time frame. Select the dates that you want to view from the calendar menu.
<b>Last 7 Days</b>	All of the incidents that were reported in the previous seven days.
<b>Last 30 Days</b>	All of the incidents that were reported in the previous 30 days.
<b>Last Month</b>	All of the incidents that were reported during the previous calendar month.
<b>Last Week</b>	All of the incidents that were reported during the previous calendar week.
<b>Last Quarter</b>	All of the incidents that were reported during the previous quarter.
<b>Last Year</b>	All of the incidents that were reported during the last calendar year.
<b>Today</b>	All of the incidents that were reported today.
<b>Yesterday</b>	All of the incidents that were reported yesterday.

**Table 37-3** 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, and Discover incidents.

**Table 37-3** General filters for severity values

Name	Description
<b>High</b>	Lists only the high-severity incidents. Displays how many high-severity incidents are in the incident list.
<b>Info</b>	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.
<b>Low</b>	Lists only the low-severity incidents. Displays how many low-severity incidents are in the incident list.
<b>Medium</b>	Lists only the medium-severity incidents. Displays how many medium-severity incidents are in the incident list.

[Table 37-4](#) lists the general filter options for Network Discover scans. This filter is only available for Discover incidents.

**Table 37-4** General filters for scans

Name	Description
<b>All Scans</b>	All of the incidents that have been reported in all of the scans that have been run.
<b>Initial Scan</b>	All of the incidents that were reported in the initial scan.
<b>In Process</b>	All of the incidents that have been reported in the scans that are currently in progress.
<b>Last Completed Scan</b>	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 37-5](#) lists the general filter options by detection date for Discover incidents.

**Table 37-5** General filters by date

Name	Description
<b>All Dates</b>	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.

**Table 37-5** General filters by date (*continued*)

Name	Description
<b>Current Quarter to Date</b>	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.
<b>Current Year to Date</b>	All of the incidents that have been reported for the current year up to today's date.
<b>Custom</b>	A custom time frame. Select the dates that you want to view from the calendar menu.
<b>Custom Since</b>	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.
<b>Custom Before</b>	The Symantec DLP Agents that have connected to an Endpoint Server before a specific date. Select the final date for the filter.
<b>Last 7 Days</b>	All of the incidents that were reported in the previous seven days.
<b>Last 30 Days</b>	All of the incidents that were reported in the previous 30 days.
<b>Last Month</b>	All of the incidents that were reported during the previous calendar month.
<b>Last Week</b>	All of the incidents that were reported during the previous calendar week.
<b>Last Quarter</b>	All of the incidents that were reported during the previous quarter.
<b>Last Year</b>	All of the incidents that were reported during the last calendar year.
<b>Today</b>	All of the incidents that were reported today.
<b>Yesterday</b>	All of the incidents that were reported yesterday.

## 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 37-6](#), [Table 37-7](#), and [Table 37-8](#) list the advanced filter options for reports.

**Table 37-6**      Advanced filters, first field

Name	Description	Applicable products
<b>Agent Configuration</b>	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

**Table 37-6**      Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>Agent Configuration Status</b>		Endpoint

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
	<p>Summarize the agent by the status of the configuration entity.</p> <p>Depending on whether you are implementing the agent configuration models through the Enforce administration console or the Symantec Management Platform (SMP) console, the Agent Configuration Status results vary.</p> <p>The following results are applicable if you deploy the entities through the Enforce console:</p> <ul style="list-style-type: none"> <li>■ <b>Current Configuration</b> The configuration on the agent is the same as the configuration on the Endpoint Server.</li> <li>■ <b>Outdated Configuration</b> The configuration on the agent is different than the configuration on the Endpoint Server.</li> <li>■ <b>Unknown/deleted Configuration</b> The agents either cannot report which configuration is installed, or the configuration on the agent has been deleted from the Endpoint Server.</li> </ul> <p>The following results are applicable if you deploy the entities through SMP:</p> <ul style="list-style-type: none"> <li>■ <b>Current Configuration</b> The named configuration on the Endpoint Server has not changed since it was sent to the agent.</li> <li>■ <b>Outdated Configuration</b> The named configuration on the Endpoint Server has</li> </ul>	

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
	<p>changed since it was sent to the agent.</p> <ul style="list-style-type: none"> <li>■ Unknown/deleted Configuration</li> </ul> <p>The agents either cannot report which configuration is installed, or the named configuration has been deleted from the system.</p>	
<b>Agent Response</b>	Filter incidents by how the agent has responded to the incident.	Endpoint
<b>Application Name</b>	Filter the incidents by the name of the application where the incident was generated.	Endpoint
<b>Application Window Title</b>	Filter the incidents by a string in the title of the window where the incident was generated.	Endpoint
<b>Attachment File Name</b>	Filter incidents by the file name of the attachment that is associated with the incident.	Network
<b>Attachment File Size</b>	Filter incidents by the size of the attachment that is associated with the incident.	Network
<b>Content Root</b>	Filter the incidents by the content root path.	Discover
<b>Data Owner Email Address</b>	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

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>Data Owner Name</b>	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.  See <a href="#">“Creating and distributing aggregated incident reports to data owners”</a> on page 788.	Network Endpoint Discover
<b>Destination IP</b>	Filter the incidents by the destination IP address for the message that generated the incident.	Network Endpoint
<b>Detection Date</b>	Filter the incidents by the date that the incident was detected.	Discover
<b>Device Instance ID</b>	Summarize the incidents by the specific device that created the violation.	Endpoint
<b>Document Name</b>	Filter the incidents by the name of the violating document.	Discover
<b>Domain</b>	Filter the incidents by the domain name that is associated with the incident.	Network
<b>Endpoint Location</b>	Filter the incidents by the endpoint location.  The location can be one of the following:  <ul style="list-style-type: none"> <li>■ On the Corporate Network</li> <li>■ Off the Corporate Network</li> </ul>	Endpoint
<b>File Last Modified Date</b>	Filter the incidents by the last date when the file was modified.	Endpoint Discover
<b>File Location</b>	Filter the incidents by the location of the violating file.	Endpoint

**Table 37-6**      Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>File Name</b>	Filter the incidents by the name of the violating file. No wildcards, but you can specify a partial match, for example <code>.pdf</code> .	Endpoint Discover
<b>File Owner</b>	Filter the incidents by the owner of the violating files.	Discover
<b>File Size</b>	Filter the incidents by the size of the violating file.	Endpoint Discover
<b>Incident History Issuer</b>	Filter the incidents by the user responsible for issuing the history of the incident.	Network Endpoint Discover
<b>Incident ID</b>	Filter the incidents by the ID of the incidents.	Network Endpoint Discover
<b>Incident Match Count</b>	Filter the incidents by the number of incident matches.	Network Endpoint Discover
<b>Incident Notes</b>	Filter the incidents by a string in the incident notes.	Network Endpoint Discover
<b>Incident Reported On</b>	Filter the incidents by the date that the incident was reported.	Endpoint
<b>Investigating State</b>	Filter the agents by the investigation state. You can select one of the following: <ul style="list-style-type: none"> <li>■ Investigating</li> <li>■ Not Investigating</li> </ul>	Discover Endpoint
<b>Last Connection Time</b>	Filter agents according to the last time each agent connected to the Endpoint Server.	Endpoint

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>Location</b>	Filter the incidents by their location. Location can include the server where the incidents were generated.	Discover
<b>Machine IP (Corporate)</b>	Filter the incidents by the IP address of the computer on which the incidents were created.	Endpoint
<b>Machine Name</b>	Filter the incidents by the computer name on which the incidents were created.	Endpoint
<b>Network Prevent Action</b>	Filter the incidents by the action from Network Prevent.	Network
<b>Policy</b>	Filter the incidents by the policy from which they were created.	Network Endpoint Discover
<b>Policy Group</b>	Filter the incidents by the policy group to which they belong.	Network Endpoint Discover
<b>Policy Rule</b>	Filter the incidents by the policy rule that generated the incidents.	Network Endpoint Discover
<b>Protect Status</b>	Filter the incidents by the Network Protect status of the incidents.	Discover
<b>Protocol</b>	Filter the incidents by the protocol to which they belong.	Network
<b>Protocol or Endpoint Destination</b>	Filter the incidents by the protocol or the endpoint destination that generated the incident.	Endpoint
<b>Read ACL: File</b>	Filter the incidents by the File access control list.	Endpoint Discover
<b>Read ACL: Share</b>	Filter the incidents by the Share access control list.	Discover

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>Recipient</b>	Filter the incidents by the name of the recipient of the message that generated the incident.	Network Endpoint Discover
<b>Scanned Machine</b>	Filter the incidents by the computers that have been scanned.	Discover
<b>Seen Before</b>	Filter the incidents on whether an earlier connected incident exists.	Discover, but not for SQL Database incidents (where <b>Seen Before</b> is always false)
<b>Sender</b>	Filter the incidents by the sender.	Network Endpoint Discover
<b>Server</b>	Filter the incidents by the server on which they were created.	Network Endpoint Discover
<b>SharePoint ACL: Permission Level</b>	Filter the incidents on the permission level of the SharePoint access control list.	Discover
<b>SharePoint ACL: User/Group</b>	Filter the incidents on the user or group in the SharePoint access control list.	Discover
<b>Source IP</b>	Filter the incidents by the source IP address from which they were created.	Network
<b>Subject</b>	Filter incidents by the subject line of the message that generated the incident.	Network Discover
<b>Superseded</b>	Summarize the incidents by the incident responses have been superseded by other responses.	Discover Endpoint
<b>Target Type</b>	Filter the incidents by the type of target that is associated with the incidents.	Discover

**Table 37-6** Advanced filters, first field (*continued*)

Name	Description	Applicable products
<b>Time Since First Detected</b>	Filter the incidents by how much time has passed since the incident was first detected.	Discover, but not for SQL Database incidents
<b>URL</b>	Filter the incidents by the URL where the violations occurred.	Discover
<b>User Justification</b>	Filter the incidents by the justification that was input by the user.	Endpoint
<b>User Name</b>	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 37-7** Advanced filters, second field

Name	Description
<b>Contains Any Of</b>	Lets you modify the filter to include any words in the text string, or lets you choose from a list in the third field.
<b>Contains Ignore Case</b>	Lets you modify the filter to ignore a specific text string.
<b>Does Not Contain Ignore Case</b>	Lets you modify the filter to filter out the ignored text string.
<b>Does Not Match Exactly</b>	Lets you modify the filter to match on any combination of the text string.
<b>Ends with Ignore Case</b>	Lets you modify the filter so that only the incidents that end with the ignored text string appear.
<b>Is Any Of</b>	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.
<b>Is None Of</b>	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.
<b>Matches Exactly</b>	Lets you modify the filter to match exactly the text string.
<b>Matches Exactly Ignore Case</b>	Lets you modify the filter so that the filter must match the ignored text string exactly.

**Table 37-7** Advanced filters, second field (*continued*)

Name	Description
<b>Starts with Ignore Case</b>	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 `.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 reports”](#) on page 777.

[Table 37-8](#) lists some of the options in the third field.

**Table 37-8** Advanced filters, third field

Name	Description
<b>Blocked</b>	The user was blocked from performing the action that cause the incident.
<b>Content Removed</b>	The content in violation was removed.
<b>No Remediation</b>	No incident remediation has occurred for this incident.
<b>None</b>	No action was taken regarding the violation that caused the incident.
<b>Protect File Copied</b>	The file in violation was copied to another location.
<b>Protect File Quarantined</b>	The file in violation was quarantined to another location.
<b>User Notified</b>	The user was notified that a violation had occurred.

## Summary options for reports

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.

[Table 37-9](#) lists the summary options for reports.

**Table 37-9** Summary filters

Name	Description	Applicable products
<b>Agent Configuration</b>	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
<b>Agent Response</b>	Summarize incidents by how the agent has responded to the incident.	Endpoint
<b>Content Root</b>	Summarize the incidents by the content root path.	Discover
<b>Data Owner Email Address</b>	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
<b>Data Owner Name</b>	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.  See <a href="#">“Creating and distributing aggregated incident reports to data owners”</a> on page 788.	Network Endpoint Discover
<b>Destination IP</b>	Summarize the incidents by the destination IP address.	Network Endpoint

**Table 37-9** Summary filters (*continued*)

Name	Description	Applicable products
<b>Detection Month</b>	Summarize the incidents by the month in which they were detected.	Discover
<b>Detection Quarter</b>	Summarize the incidents by the calendar quarter in which they were detected.	Discover
<b>Detection Week</b>	Summarize the incidents by the week in which they were detected.	Discover
<b>Detection Year</b>	Summarize the incidents by the year in which they were detected.	Discover
<b>Device Instance ID</b>	Summarize the incidents by the specific device that created the violation.	Endpoint
<b>Domain</b>	Summarize the incidents by the domain name.	Network
<b>Endpoint Location</b>	Summarize the incidents by the location of the endpoint.  The location can be one of the following:  ■ <b>On the Corporate Network</b> ■ <b>Off the Corporate Network</b>	Endpoint
<b>File Name</b>	Summarize the incidents by the file name that is associated with the incident.	Endpoint
<b>File Owner</b>	Summarize the incidents by the owner of the file.	Discover
<b>Investigating State</b>	Summarize the agents by the current status.	Endpoint Discover
<b>Location</b>	Summarize the incidents by their location.	Discover
<b>Machine IP (Corporate)</b>	Summarize the incidents by the IP address of a machine on the corporate network.	Endpoint

Table 37-9 Summary filters (*continued*)

Name	Description	Applicable products
<b>Machine Name</b>	Summarize the incident by the computer name on which the incidents were created.	Endpoint
<b>Month</b>	Summarize the incidents by the month in which they were created.	Network Endpoint
<b>Months Since First Detected</b>	Summarize the incidents by how many months have passed since the incident was first detected.	Discover
<b>Network Prevention Action</b>	Summarize the incidents by the action from Network Prevent.	Network
<b>No primary summary selected</b>	Placeholder selection to denote that no primary summary has been selected.	Network Endpoint Discover
<b>No secondary summary selected</b>	Placeholder selection to denote that no summary has been selected.	Network Endpoint Discover
<b>Policy</b>	Summarize the incidents by the policy from which they were created.	Network Endpoint Discover
<b>Policy Group</b>	Summarize the incidents by the policy group to which they belong.	Network Discover
<b>Protect Status</b>	Summarize the incidents by the Network status of the incidents.	Discover
<b>Protocol</b>	Summarize the incidents by the protocol that generated the incident.	Network
<b>Protocol or Endpoint Destination</b>	Summarize the incidents by the protocol or the endpoint destination where the incidents were created.	Endpoint

**Table 37-9** Summary filters (*continued*)

Name	Description	Applicable products
<b>Quarantine Failure Reason</b>	Summarize the incidents by the reason that the quarantine response action failed.	Endpoint Discover
<b>Quarter</b>	Summarize the incidents by the quarter in which they were created.	Network Endpoint
<b>Quarters Since First Detected</b>	Summarize the incidents by how many quarters have passed since the incident was first detected.	Discover
<b>Recipient</b>	Summarize the incidents by the recipient.	Discover
<b>Scan</b>	Summarize the incidents by which scan was used to find the incidents.	Discover
<b>Scanned Machine</b>	Summarize the incidents by the computers that have been scanned.	Discover
<b>Sender</b>	Summarize the incidents by the sender.	Network Endpoint Discover
<b>Server</b>	Summarize the incidents by the server on which they were created.	Network Endpoint
<b>Source IP</b>	Summarize the incidents by the source IP address from which they were created.	Network Endpoint
<b>Source File</b>	Summarize the incidents by the source file that violated the policy.	Endpoint
<b>Status</b>	Summarize the incidents by the incident status.	Network Endpoint Discover
<b>Subject</b>	Summarize the incidents by the subject.	Discover
<b>Target ID</b>	Summarize the incidents by the target scan ID.	Discover

**Table 37-9** Summary filters (*continued*)

<b>Name</b>	<b>Description</b>	<b>Applicable products</b>
<b>Target Type</b>	Summarize the incidents by the type of target on which the incident was generated.	Discover
<b>User Justification</b>	Summarize the incidents by the justification that was input by the user.	Endpoint
<b>User Name</b>	Summarize the incidents by the user who generated the incident.	Endpoint
<b>Week</b>	Summarize the incidents by the week in which they were created.	Network Endpoint
<b>Weeks Since First Detected</b>	Summarize the incidents by how many weeks have passed since the incident was first detected.	Discover
<b>Year</b>	Summarize the incidents by the year in which they were created.	Network Endpoint
<b>Years Since First Detected</b>	Summarize the incident by how many years have passed since the incident was first detected.	Discover



# About incident remediation

This chapter includes the following topics:

- [About incident remediation](#)
- [Viewing incidents](#)
- [Remediating incidents](#)
- [Creating and distributing aggregated incident reports to data owners](#)

## 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 38-1](#) describes the options that are involved in incident remediation:

**Table 38-1** Options involved in incident remediation

Remediation options	Description
Role-based access control	<p>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.</p> <p>See <a href="#">“About role-based access control”</a> on page 77.</p>
Severity level assignment	<p>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.</p>
Custom attribute lookup	<p>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.</p> <p>For example, you can use custom attributes as input to subsequent automated responses to automatically notify the sender's manager about the policy violation.</p> <p>See <a href="#">“Setting the values of custom attributes”</a> on page 799.</p>

**Table 38-1** Options involved in incident remediation (*continued*)

Remediation options	Description
Automated incident responses	<p>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.</p> <p>See <a href="#">“Configuring response rule actions”</a> on page 699.</p>
<b>Smart Response</b>	<p>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.</p> <p>See <a href="#">“Configuring response rule actions”</a> on page 699.</p> <p>The following standard <b>SmartResponse</b> actions are available:</p> <ul style="list-style-type: none"> <li>■ Add Note</li> <li>■ Log to a Syslog Server</li> <li>■ Send Email Notification</li> <li>■ Set Status</li> </ul> <p>In addition, <b>SmartResponse</b> manual actions are available with the Solution Packs, and with the custom FlexResponse Platform.</p>
Distribution of aggregated incident reports	<p>You can create and automatically distribute aggregated incident reports to data owners for remediation.</p> <p>See <a href="#">“Creating and distributing aggregated incident reports to data owners”</a> on page 788.</p>

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.

## 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

- 1 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 755.

- 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.

- 4 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.

- 5 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 787.

## Remediating incidents

When you remediate an incident, you can perform one of 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.
- Perform some combination of these actions.
- Remediate incidents by going to an incident list or incident snapshot and selecting actions to perform on one or more incidents.

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 786.

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 680.

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.

## Creating and distributing aggregated incident reports to data owners

You can create and automatically distribute aggregated incident reports to data owners for remediation.

An automatic workflow can be set up for the following use cases:

- Automatically or manually set the **Data Owner Name** and **Data Owner Email Address** for new incidents.

## Creating and distributing aggregated incident reports to data owners

- Set a custom status value or custom attribute to mark that the **Data Owner Name** for an incident has been verified. Custom attributes and custom status values can also mark incidents for other workflow steps.
- Set up a recurring email schedule.  
Reports can be configured to be sent on a recurring schedule, sending only the incidents that have not yet been distributed.
- Mark the incident as sent.  
After the report is sent, the status attributes and custom attributes can optionally be set, to flag the incidents for the next stage of the workflow.
- Automate the tasks.  
Lookup plug-in scripts and chained lookup plug-ins can automate the tasks in the workflow sequence.

The following process describes a complex use case that includes the setup tasks, and suggestions to automate some steps in the process.

**Table 38-2**      Setting up, creating, and distributing aggregated incident reports to data owners

Step	Action	Description
Step 1	Install and set up the Symantec Data Insight Management Server.  Make sure that the Symantec Data Insight Management Server has access to the files or file systems of interest.	See the following Symantec Data Insight documentation: <ul style="list-style-type: none"> <li>■ <i>Symantec Data Insight Installation Guide</i></li> <li>■ <i>Symantec Data Insight Administrator's Guide</i></li> </ul>
Step 2	Install the Symantec Data Loss Prevention product, including at least one Network Discover Server.	See the <i>Symantec Data Loss Prevention Installation Guide</i> .
Step 3	Set up the connection between the Enforce Server and the Symantec Data Insight Management Server.	<b>Note:</b> Symantec Data Insight is a separately licensed option. If Symantec Data Insight is not licensed on the Enforce Server, the menu option to configure the connection to the Symantec Data Insight Management Server does not appear.
Step 4	Test the connection from the Enforce Server to the Symantec Data Insight Management Server.	

**Table 38-2** Setting up, creating, and distributing aggregated incident reports to data owners (*continued*)

Step	Action	Description
Step 5	On the Enforce Server, create a custom status value or custom attribute for the Data Owner Name verification, and any workflow status attributes.	See “ <a href="#">About incident status attributes</a> ” on page 793.
Step 6	Map the details from the Symantec Data Insight Management Server into the custom attributes that you created.	Edit the properties file for Symantec Data Insight on the Enforce Server, to map the details from the Symantec Data Insight Management Server into the custom attributes that you created.
Step 7	Map any of the Symantec Data Insight attributes directly into the <b>Data Owner Name</b> field.	To map the Symantec Data Insight data user (the person who uses the file most frequently) to the <b>Data Owner Name</b> , set the <code>Data_User</code> parameter.
Step 8	<p>Set up all your lookup plug-ins.</p> <p>For example, you may want to chain the LDAP Lookup Plug-In to take the <b>Data Owner Name</b> and set the <b>Data Owner Email Address</b> as either the data owner or the manager of the data owner.</p> <p>No built-in capability provides consistency between the data owner and email address. This action must be customized.</p> <p>The <b>Data Owner Email Address</b> can have multiple email addresses that are separated with commas.</p> <p><b>Note:</b> If duplicate attribute names exist between these names and custom attributes, then both fields are updated.</p>	<p>Edit the <code>Plugins.properties</code> file to set up all your lookup plug-ins.</p> <p>See the <i>Symantec Data Loss Prevention Lookup Plug-in Guide</i>.</p>

**Table 38-2**      Setting up, creating, and distributing aggregated incident reports to data owners *(continued)*

Step	Action	Description
Step 9	Verify that the Enforce Server general settings are set up to send email notifications.	<p>Set up the SMTP notification settings.</p> <p>Set the option <b>Send report data with emails</b>.</p> <p>See <a href="#">“Configuring the Enforce Server to send email alerts”</a> on page 115.</p>
Step 10	Verify that the incident responder has the privileges to run the reports.	<p>The <b>Remediate Incidents</b> privilege is required to configure and run the reports.</p> <p>The <b>Lookup Attributes</b> privilege is required to set attributes from the lookup plug-ins.</p> <p>The User Privilege <b>CSV Attachment in Email Reports</b> is required to attach the CSV report to the email.</p> <p>See <a href="#">“About role-based access control”</a> on page 77.</p>
Step 11	Set up a Network Discover and run a sample scan of the file systems of interest.	See <a href="#">“Setting up scans of file shares”</a> on page 899.
Step 12	Set up any custom reports.	<p>Set up a filtered report, or set up any report that you want to distribute. For example, you can filter based on the new incidents.</p> <p>Select the option <b>Change Incident Status / Attributes</b> of the reports scheduling to set incident status or attributes when the email is sent.</p> <p>See <a href="#">“Scheduling custom incident reports”</a> on page 756.</p> <p>You can also manually set the custom attribute that indicates these incidents were verified. Select any or all incidents in the list. Use the drop-down <b>Incident Actions</b> and select <b>Set Attributes</b>. You can also set a custom status from this drop-down menu.</p>

**Table 38-2**      Setting up, creating, and distributing aggregated incident reports to data owners *(continued)*

Step	Action	Description
Step 13	Save the custom reports and set up a distribution schedule.	See <a href="#">“Saving custom incident reports”</a> on page 755. See <a href="#">“Scheduling custom incident reports”</a> on page 756.

# Managing custom attributes and status values for incidents

This chapter includes the following topics:

- [About incident status attributes](#)
- [Configuring status attributes and values](#)
- [Configuring status groups](#)
- [About custom attributes](#)
- [Setting the values of custom attributes](#)
- [Configuring custom attributes](#)

## 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 795.

#### ■ **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 796.

#### ■ **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 797.

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 795.

See [“About incident remediation”](#) on page 783.

See [“About custom attributes”](#) on page 797.

## 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 style="list-style-type: none"> <li>■ Click <b>[up]</b> to move an attribute up in the order.</li> <li>■ Click <b>[down]</b> to move an attribute down in the order.</li> </ul>

### To create a new incident status attribute

- 1 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.
- 4 Click **Save**.

See “[Configuring status groups](#)” on page 796.

See “[About incident status attributes](#)” on page 793.

## 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 <b>Add Status Group</b> 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 style="list-style-type: none"><li>■ Click <b>[up]</b> to move a group up in the order.</li><li>■ Click <b>[down]</b> to move a group down in the order.</li></ul>

### To define a new status group

- 1 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.

- 4 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 795.

- 5 Click **Save**.

See [“Configuring status attributes and values”](#) on page 795.

See [“About incident status attributes”](#) on page 793.

## 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 793.
- **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:

<b>Action</b>	<b>Procedure</b>
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 drop-down menus.	<ol style="list-style-type: none"><li>1 Click <b>[up]</b> to move an attribute up in the order.</li><li>2 Click <b>[down]</b> to move an attribute down in the order.</li></ol>
Reload Lookup Plug-ins	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 style="list-style-type: none"><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 793.

See [“Configuring custom attributes”](#) on page 799.

See [“Setting the values of custom attributes”](#) on page 799.

See the *Symantec Data Loss Prevention Lookup Plug-in Guide* for detailed information about custom attributes and lookup plug-ins.

## Setting the values of custom attributes

You can specify incident remediation status or workflow progress with values in custom attributes.

### 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.
- 4 When you are finished setting values, click **Save**.

## Configuring custom attributes

Use the **Configure Custom Attribute** screen to add or modify the a custom attribute.

### To create a new custom attribute

- 1 Go to the **Attributes** screen (**System > Incident Data > Attributes**) screen.
- 2 Click the **Custom Attributes** tab.
- 3 Click the **Add** button.
- 4 Enter a name for the new custom attribute.
- 5 If the value for this attribute is an email address, check the **Is Email Address** box.
- 6 Select an attribute group for this new custom attribute:
  - Click on a group name in the **Attribute Group** drop-down list.
  - If you need to create a new attribute group, click **Create New Attribute Group** in the drop-down list. Then fill in the name for the new attribute group.
- 7 Click **Save**.

See [“About incident status attributes”](#) on page 793.

See [“Configuring status groups”](#) on page 796.

See [“Configuring status attributes and values”](#) on page 795.



# Monitoring and preventing data loss in the network

- [Chapter 40. Implementing Network Monitor](#)
- [Chapter 41. Implementing Network Prevent \(Email\)](#)
- [Chapter 42. Implementing Network Prevent \(Web\)](#)



# Implementing Network Monitor

This chapter includes the following topics:

- [Implementing 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.

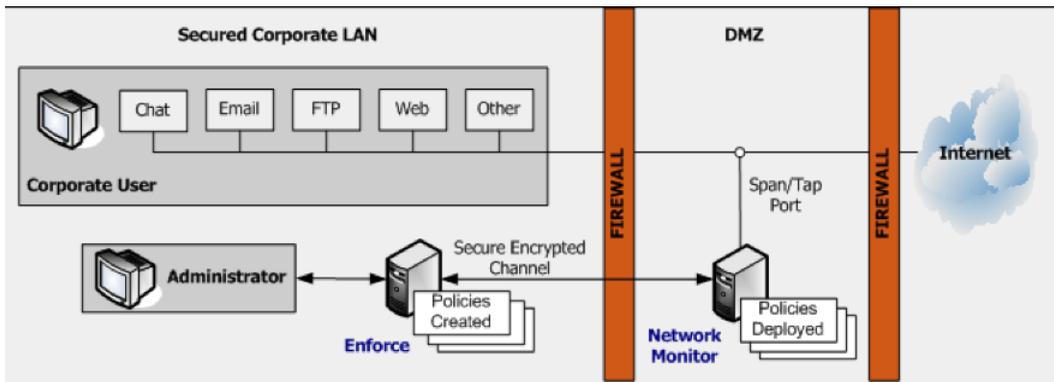
To monitor network traffic, a Network Monitor Server requires:

- 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 Endace DAG network measurement card (Endace card) 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.)

- 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 an Endace card, the card must use the correct driver.  
See [“Choosing a network packet capture method”](#) on page 805.

**Figure 40-1** 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 805.
- 3 Install the necessary NIC or Endace card 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 Endace card must operate in promiscuous mode so that it picks up all inbound and all outbound traffic.  
See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about supported NICs and Endace cards.
- 4 On a Windows platform, install WinPcap if it is not already installed.  
See [“Installing WinPcap on a Windows platform”](#) on page 806.
- 5 If necessary, update the Endace driver.  
See [“Updating the Endace card driver”](#) on page 807.

- 6 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.

---

- 7 Use a protocol analyzer such as Wireshark to validate traffic on the tap or SPAN that feeds into your NIC or Endace card.
- 8 Configure the Network Monitor Server.  
See [“Configuring the Network Monitor Server”](#) on page 807.
- 9 Create and deploy a test policy for Network Monitor.  
See [“Creating a policy for Network Monitor”](#) on page 810.
- 10 Test the system by generating an incident against your test policy.  
See [“Testing Network Monitor”](#) on page 810.

## 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 806.
- 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.

- Endace card on either Windows or Linux platforms. An Endace DAG network measurement card can be used on both Windows and Linux platforms to provide network packet capture in high-traffic environments. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about supported Endace cards and drivers.

**Table 40-1** Packet capture alternatives

Platform	Card	Software
Windows	NIC	WinPcap
Linux	NIC	Native
Windows and Linux	Endace	Endace

## 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.
- If you use an Endace card, in some instances you may need to update the card driver.

See [“Installing WinPcap on a Windows platform”](#) on page 806.

See [“Updating the Endace card driver”](#) on page 807.

### 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.

**To install WinPcap on the Network Monitor Server:**

- 1 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.

Additional details can be found in the *Symantec Data Loss Prevention Installation Guide*.

## Updating the Endace card driver

If you upgrade a Network Monitor Server that uses an Endace card from Symantec Data Loss Prevention version 8.x 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**

- 1 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 807.

## Configuring the Network Monitor Server

You configure the Network Monitor Server by selecting the network interface (NIC or Endace card) to use for traffic capture. You must also select which protocols to monitor.

**To configure a Network Monitor Server**

- 1 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 an Endace card for traffic capture, skip to step 6.
- 2 If you use an Endace card, click **Server Settings**.

**3** 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 <i>endace_home</i> \dag-version\bin (for example, on a Windows platform, c:\Program Files\Endace\dag-3.2.2\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 \xilinx directory.
PacketCapture.IS_ENDACE_ENABLED	Change the value to true.

- 4** 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.
- 5** Go to **System > Servers > Overview** and again click on the Network Monitor Server.
- 6** 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.
- 7** 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.
- 8** Leave the **Archive Folder** field blank.
- 9** Select one or more **Network Interfaces** (NICs or Endace cards) through which the Network Monitor Server should capture traffic.

- 10 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.

- 11 Click **Save**.
- 12 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 810.

See [“Enabling GET processing with Network Monitor”](#) on page 809.

See [“Creating a policy for Network Monitor”](#) on page 810.

## 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.

### To enable GET processing

- 1 Ensure that the **L7.processGets** advanced server setting on the Network Monitor Server **true** (which is the default).
- 2 Change the **PacketCapture.DISCARD\_HTTP\_GET** advanced server setting on the Network Monitor Server from the default setting of **true** to **false**.
- 3 Reduce the size of the **L7.minSizeofGetURL** advanced server setting on the 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.

See [“Enabling GET processing for Network Prevent \(Web\)”](#) on page 835.

## 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 [“Implementing policies”](#) on page 317.

**To create a test policy for Network Monitor**

- 1 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 697.

- 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_vontu_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 337.

See [“Configuring policies”](#) on page 338.

## Testing Network Monitor

You can test Network Monitor by sending an email that violates your test policy.

**To test your system**

- 1 Access an email account that routes messages through the MTA.
- 2 Send an email that contains confidential data. For example, send an email that contains the keyword `test_vontu_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 745.
- See [“Configuring the Network Monitor Server”](#) on page 807.
- See [“Creating a policy for Network Monitor”](#) on page 810.



# Implementing Network Prevent (Email)

This chapter includes the following topics:

- [Implementing Network Prevent \(Email\)](#)
- [About Mail Transfer Agent \(MTA\) integration](#)
- [Configuring Network Prevent \(Email\) Server for reflecting or forwarding mode](#)
- [Specifying one or more upstream mail transfer agents \(MTAs\)](#)
- [Creating a policy for Network Prevent \(Email\)](#)
- [About policy violation data headers](#)
- [Enabling policy violation data headers](#)
- [Testing Network Prevent \(Email\)](#)

## Implementing Network Prevent (Email)

Network Prevent (Email) monitors and analyzes outbound email traffic in-line and (optionally) blocks, redirects, or modifies email messages as specified in your policies. Network Prevent (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 (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.

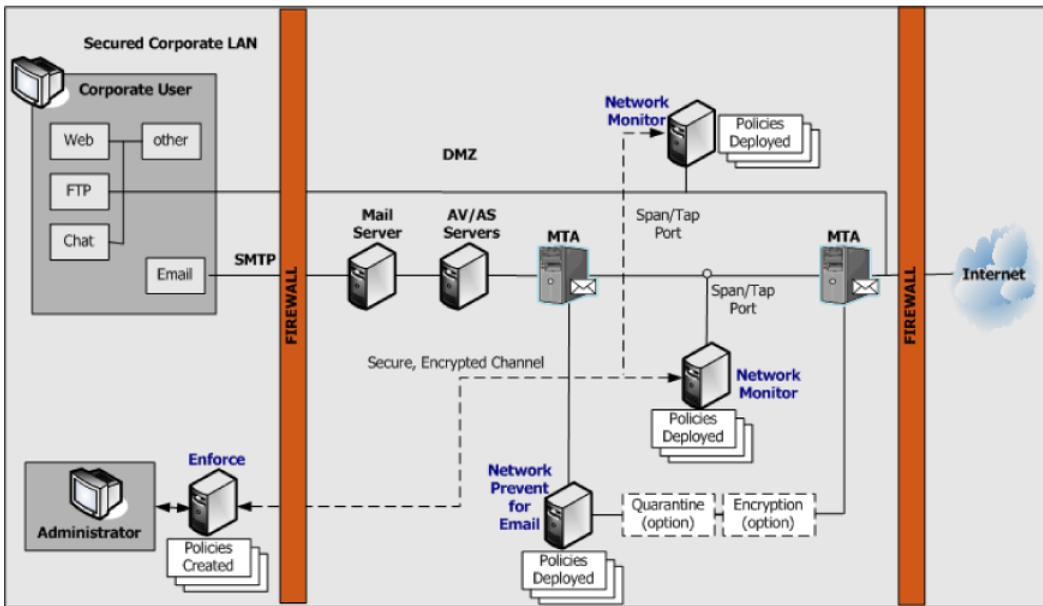
---

**Note:** Review the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)* to determine your preferred integration architecture before you continue with the implementation.

---

Figure 41-1 shows an integration of Network Prevent (Email) Server with a next-hop MTA that you manage in the network. As an alternative, you can integrate Network Prevent (Email) Server with a hosted email server that resides outside the firewall.

**Figure 41-1** A basic Network Prevent (Email) setup



First, you need to know the high-level steps that are required for implementing Network Prevent (Email). You can check the cross-referenced sections for more details.

### To implement Network Prevent (Email)

- 1 Choose an integration architecture and configure your Mail Transfer Agent (MTA) to work with the Network Prevent (Email) Server.  
See [“About Mail Transfer Agent \(MTA\) integration”](#) on page 815.
- 2 Configure the Network Prevent (Email) Server to work within your chosen integration architecture.  
See [“Configuring Network Prevent \(Email\) Server for reflecting or forwarding mode”](#) on page 816.
- 3 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.
- 4 Create and deploy a policy for Network Prevent (Email).  
See [“Creating a policy for Network Prevent \(Email\)”](#) on page 822.
- 5 Test the system by generating an incident against your test policy.  
See [“Testing Network Prevent \(Email\)”](#) on page 825.

## About Mail Transfer Agent (MTA) integration

Choose an integration architecture and configure your Mail Transfer Agent (MTA) to work with the Network Prevent (Email) Server.

Review the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)*. Familiarize yourself with the compatible integration architectures.

The Network Prevent (Email) Server can operate with your MTA in either reflecting or forwarding modes:

- **Reflecting mode.** In reflecting mode, the Network Prevent (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 (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 (Email) Server configuration.

You can also configure a single Network Prevent (Email) Server to work with multiple MTAs.

See [“Specifying one or more upstream mail transfer agents \(MTAs\)”](#) on page 821.

## Configuring Network Prevent (Email) Server for reflecting or forwarding mode

Use the following instructions to configure Network Prevent (Email) Server to operate either in reflecting or forwarding mode.

### To configure the Network Prevent (Email) Server

- 1 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.
- 3 Click the name of the Network Prevent (Email) Server that you want to configure.
- 4 Click **Configure**.
- 5 Deselect **Trial Mode** to enable blocking of email messages that are found to violate Symantec Data Loss Prevention policies.

**6** Configure reflecting mode or forwarding mode by modifying the following fields:

<b>Field</b>	<b>Description</b>
<b>Next Hop Configuration</b>	<p>Select <b>Reflect</b> to operate Network Prevent (Email) Server in reflecting mode. Select <b>Forward</b> to operate in forwarding mode.</p> <p><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.</p>
<b>Enable MX Lookup</b>	<p>This option applies only to forwarding mode configurations.</p> <p>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 (Email) Server uses the returned MX records to select the address of the next hop mail server.</p> <p>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:</p> <p style="margin-left: 20px;"><code>companyname.com</code></p> <p>Network Prevent (Email) Server performs MX record queries for the domain names that you specify.</p> <p><b>Note:</b> You must include at least one valid entry in the <b>Enter Domains</b> text box to successfully configure forwarding mode behavior.</p>

Field	Description
<b>Disable MX Lookup</b>	<p>This field applies only to forwarding mode configurations.</p> <p>Select <b>Disable MX Lookup</b> if you want to specify the exact hostname or IP address of one or more next-hop MTAs. Network Prevent (Email) Server uses the hostnames or addresses that you specify and does not perform an MX record lookup.</p> <p>If you select <b>Disable MX Lookup</b>, also add one or more hostnames or IP addresses for next-hop MTAs in the <b>Enter Hostnames</b> text box. You can specify multiple entries by placing each entry on a separate line. For example:</p> <pre>smtpl .companyname .com smtp2 .companyname .com smtp3 .companyname .com</pre> <p>Network Prevent (Email) Server always tries to proxy to the first MTA that you specify in the list. If that MTA is not available, Network Prevent (Email) Server tries the next available entry in the list.</p> <p><b>Note:</b> You must include at least one valid entry in the <b>Enter Hostnames</b> text box to successfully configure forwarding mode behavior.</p>

7 Click **Save**.

**8** Click **Server Settings** to verify or configure these advanced settings:

<b>Field</b>	<b>Description</b>
<b>RequestProcessor.ServerSocketPort</b>	<p>Ensure that this value matches the number of the SMTP Listener port to which the upstream MTA sends email messages. The default is 10025.</p> <p><b>Note:</b> Many Linux systems restrict ports below 1024 to root access. Network Prevent (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 (Email) port (port 10025 by default).</p> <p>See <a href="#">“Configuring Linux IP tables to reroute traffic from a restricted port”</a> on page 820.</p>
<b>RequestProcessor.MTAResubmitPort</b>	<p>Ensure that this value matches the number of the SMTP Listener port on the upstream MTA to which the Network Prevent (Email) Server returns mail. The default is 10026.</p>
<b>RequestProcessor.AddDefaultHeader</b>	<p>By default, Network Prevent (Email) Server uses a header to identify all email messages that it has processed. The header and value are specified in the <b>RequestProcessor.DefaultPassHeader</b> field.</p> <p>Change the value of this field to false if you do not want to add a header to each message.</p>

Field	Description
<b>RequestProcessor.AddDefaultPassHeader</b>	This field specifies the header and value that Network Prevent (Email) Server adds to each email message that it processes. The default header and value is <code>X-Filter-Loop: Reflected</code> . 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 <b>AddDefaultPassHeader</b> field to <code>False</code> .

---

**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 (Email) Server must authenticate itself to the upstream MTA, and the next-hop MTA must authenticate itself to Network Prevent (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 821.

See [“Creating a policy for Network Prevent \(Email\)”](#) on page 822.

See [“Testing Network Prevent \(Email\)”](#) on page 825.

## Configuring Linux IP tables to reroute traffic from a restricted port

Many Linux systems restrict ports below 1024 to root access. Network Prevent (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 (Email) default port 10025. Then ensure that Network Prevent (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 (Email) port, enter the correct values in the `iptables` commands.

#### To configure route traffic from port 25 to port 10025

- 1 Configure Network Prevent (Email) to use the default port 10025 if necessary. See [“Configuring Network Prevent \(Email\) Server for reflecting or forwarding mode”](#) on page 816.
- 2 In a terminal window on the Network Prevent (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 (Email) Server can accept connections to the ESMTP service port from any system on the network. You can restrict Network Prevent (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 (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 (Email) Server:**

- 1 Go to **System > Servers > Overview** and click on the wanted Network Prevent (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 (Email) Server.

- 4 You can limit the systems that are allowed to connect with this Network Prevent (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.
- 5 Click **Save**.

Changes to this setting do not take effect until you restart the server.

## Creating a policy for Network Prevent (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 “[Implementing policies](#)” on page 317.

You can also incorporate the following rules, which are specific to Network Prevent (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-2822 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 (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 (Email)**

- 1 In the Enforce Server administration console, create a response rule that includes one of the actions specific to Network Prevent (Email). For example, create a response rule that includes the **Network: Block SMTP Message** action.

See [“Configuring response rules”](#) on page 697.

- 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 338.

See [“About policy violation data headers”](#) on page 824.

## 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 quarantine 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 824.

## Enabling policy violation data headers

Three multiple-policy headers can be used in combination.

To enable policy violation message headers:

- 1 Go to **System > Servers > Overview** and click on the wanted Network Prevent Server (Email).
- 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**.
- 4 Change the value to **true**.
- 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 824.

## Testing Network Prevent (Email)

You can test Network Prevent (Email) by sending an email that violates your test policy.

### To test your system

- 1 Access an email account that routes messages through an MTA that is integrated with your Network Prevent (Email) Server.
- 2 Send an email that contains confidential data. For example, send an email that contains the word *Secret*.
- 3 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 745.



# Implementing Network Prevent (Web)

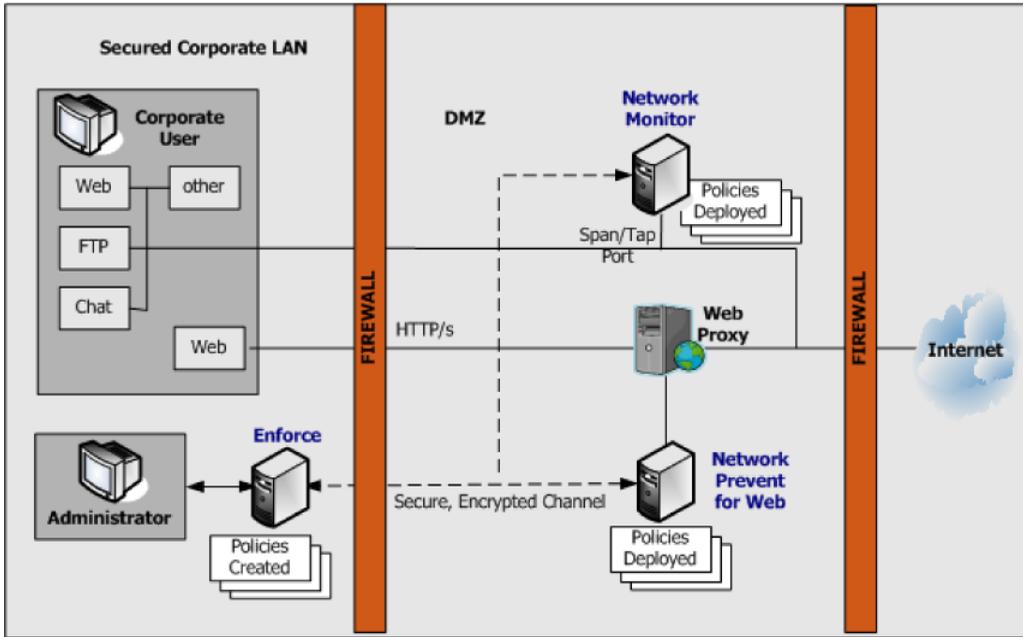
This chapter includes the following topics:

- [Implementing Network Prevent \(Web\)](#)
- [Configuring Network Prevent \(Web\) Server](#)
- [About proxy server configuration](#)
- [Specifying one or more proxy servers](#)
- [Enabling GET processing for Network Prevent \(Web\)](#)
- [Creating policies for Network Prevent \(Web\)](#)
- [Testing Network Prevent \(Web\)](#)
- [Troubleshooting information for Network Prevent \(Web\) Server](#)

## Implementing Network Prevent (Web)

The Network Prevent (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 42-1 A basic Network Prevent (Web) setup



First, you need to know the high-level steps that are required for implementing Network Prevent (Web). You can check the cross-referenced sections for more details.

#### To implement Network Prevent (Web)

- 1 Make sure the Network Prevent (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 \(Web\) Server”](#) on page 829.
- 2 Configure your HTTP proxy server to work with the Network Prevent (Web) Server.  
See [“About proxy server configuration”](#) on page 832.
- 3 Create and deploy a policy for Network Prevent (Web).  
See [“Creating policies for Network Prevent \(Web\)”](#) on page 836.

- 4 Test the system by generating an incident against your test policy.  
See [“Testing Network Prevent \(Web\)”](#) on page 838.
- 5 If required, troubleshoot the implementation.  
See [“Troubleshooting information for Network Prevent \(Web\) Server”](#) on page 838.

## Configuring Network Prevent (Web) Server

You can use a number of configuration options for Network Prevent (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 (Web) server configuration

- 1 Go to **System > Servers > Overview** and click the Network Prevent (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**.
- 3 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.

- 4 Verify or modify the filter options for requests from HTTP clients (user agents). The options in the **Request Filtering** section are as follows:

<b>Ignore Requests Smaller Than</b>	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.
<b>Ignore Requests without Attachments</b>	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.
<b>Ignore Requests to Hosts or Domains</b>	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, <code>www.company.com</code> ), each on its own line.
<b>Ignore Requests from User Agents</b>	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, <code>java/1.4.2_xx</code> ), 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:

<b>Ignore Responses Smaller Than</b>	Specifies the minimum size of the body of HTTP responses that are inspected by this server. (Default is 4096 bytes.)
<b>Inspect Content Type</b>	<p>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 <code>application/wordperfect5.1</code> to have Symantec Data Loss Prevention analyze WordPerfect 5.1 files.</p> <p>Note that it is generally more efficient to specify MIME content types at the Web proxy level.</p>
<b>Ignore Responses from Hosts or Domains</b>	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, <code>www.company.com</code> ), each on its own line.
<b>Ignore Responses to User Agents</b>	Causes the server to ignore responses to user agents (HTTP clients) you specify. You can type one or more user agent values (for example, <code>java/1.4.2_xx</code> ), each on its own line.

- 6 Verify or modify settings for the ICAP connection between the HTTP proxy server and the Web Prevent Server. The **Connection** options are as follows:

<b>TCP Port</b>	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.
<b>Maximum Number of Requests</b>	Specifies the maximum number of simultaneous ICAP request connections from the HTTP proxy or proxies. The default is 25.
<b>Maximum Number of Responses</b>	Specifies the maximum number of simultaneous ICAP response connections from the HTTP proxy or proxies. The default is 25.
<b>Connection Backlog</b>	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.

- 7 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 Network Prevent Server (Web). The HTTP proxy acts as an ICAP client to the Network Prevent (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 (Web) Server to analyze requests. Use a second Network Prevent (Web) Server to analyze responses.

Note that most proxy servers provide methods of filtering what is forwarded to the Network Prevent (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 835.

See [“Proxy server compatibility with Network Prevent \(Web\)”](#) on page 833.

See [“Configuring request and response mode services”](#) on page 833.

## Proxy server compatibility with Network Prevent (Web)

Network Prevent (Web) Servers can operate with the following HTTP proxies:

**Table 42-1** Network Prevent (Web) supported proxy servers

Proxy	Supported protocols	Configuration information
Blue Coat ProxySG	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Blue Coat product documentation
Blue Coat NetCache proxy	HTTP, FTP over HTTP	
Cisco IronPort S-Series	HTTP, HTTPS, FTP over HTTP	Cisco IronPort product documentation
Microsoft ISA	HTTP, limited FTP over HTTP	See the <i>Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server</i>
Secure Computing Secure Web (Webwasher)	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	HTTP	See the <i>Symantec Data Loss Prevention Integration Guide for Squid Web Proxy</i>

See [“Specifying one or more proxy servers”](#) on page 835.

See [“About proxy server configuration”](#) on page 832.

## 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:**

- 1 **REQMOD.** On your proxy server, create an ICAP REQMOD service that forwards requests to the Network Prevent Server (Web). 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
```

- 2 **RESPMOD.** On your proxy server, create an ICAP RESPMOD service that forwards responses to the Network Prevent Server (Web). 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|FQDN[:port]/respmo
```

**Where:**

- *ip\_address|FQDN* identifies the Network Prevent Server (Web) using either an IP address or fully qualified domain name.
- *Port* is the port number to which Network Prevent Server (Web) listens. Specifying the port number is optional when the default ICAP port (1344) is used.
- */reqmod* is required for correct functionality in REQMOD mode.
- */respmo* 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/respmo
icap://10.66.194.45:1344/respmo
icap://netmonitor1.company.com/respmo
```

Note that the port that is specified in the ICAP service definition on the proxy must match the port on which Network Prevent Server (Web) listens.

See [“Proxy server compatibility with Network Prevent \(Web\)”](#) on page 833.

See [“About proxy server configuration”](#) on page 832.

## Specifying one or more proxy servers

By default, Network Prevent (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 (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 (Web) server ICAP service port:**

- 1 Go to **System > Servers > Overview** and click on the wanted Network Prevent (Web) Server.
- 2 On the **Server Detail** screen that appears, click **Server Settings**.
- 3 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 Network Prevent (Web) Server.

- 4 You can limit the systems that are allowed to connect with this Network Prevent (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 \(Web\)”](#) on page 833.

See [“About proxy server configuration”](#) on page 832.

## Enabling GET processing for Network Prevent (Web)

By default, Network Prevent (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 (Web)

- 1 Configure the Web proxy server to forward GET requests to the Network Monitor Server as described in your proxy server documentation.
- 2 Ensure that the **L7.processGets** advanced server setting on the Network Monitor Server must be “true” (which is the default).
- 3 Reduce the size of the **L7.minSizeofGetURL** Advanced setting on the Network Monitor 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 Network Prevent (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 809.

## Creating policies for Network Prevent (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 745.

You can also incorporate the rules that are specific to Network Prevent (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 (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 (Web)**

- 1 In the Enforce Server administration console, create a response rule that includes one of the actions specific to Network Prevent (Web). For example, create a response rule that includes the **Network Prevent: Block HTTP/HTTPS** action.

See [“Configuring response rules”](#) on page 697.

- 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 Prevent: Block HTTP/HTTPS** response rule.
- Associate it with the Default policy group.

See “[Configuring policies](#)” on page 338.

## Testing Network Prevent (Web)

You can test Network Prevent (Web) by sending a Web email that violates your test policy.

### To test your system

- 1 Open a browser that accesses the Internet through your HTTP proxy server.
- 2 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.
- 3 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.
- 4 Click on the relevant incident entry to see the complete incident snapshot.

See “[About strategies for using reports](#)” on page 747.

## Troubleshooting information for Network Prevent (Web) Server

The following table describes a common problem when using Network Prevent (Web) Server and suggests a possible solution.

**Table 42-2**      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.	<p>This is expected behavior when the Network Prevent (Web) Server is running in trial mode (the default setting). If you do not want to run in trial mode, change the setting.</p> <p>See <a href="#">“Configuring Network Prevent (Web) Server”</a> on page 829.</p>



## Discovering where confidential data is stored

- [Chapter 43. About Network Discover](#)
- [Chapter 44. Setting up and configuring Network Discover](#)
- [Chapter 45. Network Discover scan target configuration options](#)
- [Chapter 46. Managing Network Discover target scans](#)
- [Chapter 47. Managing Network Discover incident reports](#)
- [Chapter 48. Using FlexResponse custom plug-ins to remediate incidents](#)
- [Chapter 49. Setting up scans of file shares](#)
- [Chapter 50. Setting up scans of Lotus Notes databases](#)
- [Chapter 51. Setting up scans of SQL databases](#)
- [Chapter 52. Setting up scans of SharePoint servers](#)
- [Chapter 53. Setting up scans of Exchange servers](#)
- [Chapter 54. About Network Discover scanners](#)
- [Chapter 55. Setting up scanning of file systems](#)

- Chapter 56. Setting up scanning of Microsoft Exchange servers
- Chapter 57. Setting up scanning of SharePoint 2007 servers
- Chapter 58. Setting up scanning of SharePoint 2003 servers
- Chapter 59. Setting up scanning of Web servers
- Chapter 60. Setting up scanning of Documentum repositories
- Chapter 61. Setting up scanning of Livelink repositories
- Chapter 62. 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 shares (CIFS, NFS, or DFS)  
See [“Setting up scans of file shares”](#) on page 899.
- Local file systems on Windows desktops and laptops  
Local file systems on Windows, Linux, AIX, and Solaris servers  
See [“Setting up scanning of file systems”](#) on page 962.
- Lotus Notes Databases  
See [“Setting up scans of Lotus Notes databases”](#) on page 909.
- SQL Databases  
See [“Setting up scans of SQL databases”](#) on page 919.
- SharePoint 2007 and 2010 servers  
See [“Setting up scans of SharePoint servers”](#) on page 927.
- Microsoft Exchange servers  
See [“Setting up scans of Exchange repositories”](#) on page 939.
- Documentum

See [“Setting up scanning of Documentum repositories”](#) on page 1023.

- Livelink  
See [“Setting up scanning of Livelink repositories”](#) on page 1033.
- Web servers (Web sites and Web-based applications)  
See [“Setting up scanning of Web servers”](#) on page 1011.
- Microsoft Exchange  
See [“Setting up scanning of Microsoft Exchange Servers ”](#) on page 975.
- SharePoint 2007  
See [“Setting up scanning of SharePoint 2007 servers”](#) on page 991.
- SharePoint 2003  
See [“Setting up scanning of SharePoint 2003 servers”](#) on page 1003.
- 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 1041.
- 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.

See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.

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 893.

## 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 43-1](#) 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 166.

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 850.

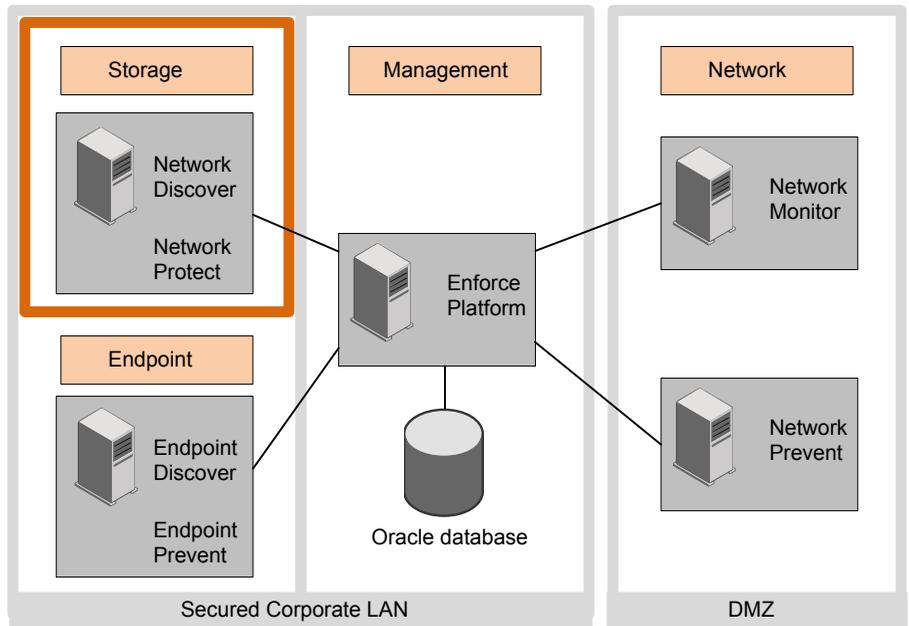
The Enforce Server also manages the scans running on the Network Discover Servers and displays the status of the scans in the user interface.

See [“Managing Network Discover target scans”](#) on page 874.

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 889.

**Figure 43-1** 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 44-1**      Setting up and Configuring Network Discover

Step	Action	Details
Step 1	Modify the Network Discover Server configuration, if needed.	See <a href="#">“Modifying the Network Discover Server configuration”</a> on page 848.

**Table 44-1**      Setting up and Configuring Network Discover (*continued*)

Step	Action	Details
Step 2	Create a policy group.	Go to <b>System &gt; Servers &gt; Policy Groups</b> . On the <b>Policy Group List</b> screen that appears, click <b>Add Policy Group</b> . See <a href="#">“Creating and modifying policy groups”</a> on page 359.
Step 3	Create a policy.	Go to <b>Manage &gt; Policies &gt; Policy List</b> on the Enforce Server. Select <b>Add a blank policy</b> . Add a rule to the policy. See <a href="#">“Configuring policies”</a> on page 338.
Step 4	Before using Network Protect for a file share Discover target, create a response rule. Using Network Protect is optional.	See <a href="#">“About response rules”</a> on page 680.
Step 5	Create a Network Discover Target.	Go to <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> on the Enforce Server. Click <b>New Target</b> , and use the pull-down menu to select the specific target type. See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 6	Set options for the target.	See <a href="#">“Network Discover scan target configuration options”</a> on page 855.
Step 7	Set up reports.	See <a href="#">“About Symantec Data Loss Prevention reports”</a> on page 745.

## 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 850.

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 883.

### To modify a Network Discover Server configuration

- 1 In the Enforce Server administration console, on the **System** menu, click **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.

- 3 Modify the server configuration.

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 hostname 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 `Vontu_home\Protect\config` (for example, `c:\Vontu\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 151.

- 4 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 886.

- 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.
- 6 To view the active scans on this Network Discover Server, on the **Policies** menu, click **Discover Scanning > Discover Servers**.

See [“Managing Network Discover target scans”](#) on page 874.

## 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 jCIFS 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 847.

## 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 847.

**To add a Network Discover target**

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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, enter the name of this Network Discover target. This name displays for management of scans.

See [“Managing Network Discover target scans”](#) on page 874.

- 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 857.

**5** Continue the addition of a new target, with the entries specific to that target type.

Network file shares (CIFS, NFS, DFS)	See <a href="#">“Setting up scans of file shares”</a> on page 899.
Lotus Notes databases	See <a href="#">“Setting up scans of Lotus Notes databases”</a> on page 909.
SQL databases	See <a href="#">“Setting up scans of SQL databases”</a> on page 919.
Local file systems on Windows desktops and laptops	See <a href="#">“Setting up scanning of file systems”</a> on page 962.
Local file systems on Windows, Linux, AIX, and Solaris servers	
Microsoft Exchange	See <a href="#">“Setting up scanning of Microsoft Exchange Servers”</a> on page 975.
SharePoint	See <a href="#">“Setting up scanning of SharePoint 2007 servers”</a> on page 991. See <a href="#">“Setting up scanning of SharePoint 2003 servers”</a> on page 1003.
Documentum	See <a href="#">“Setting up scanning of Documentum repositories”</a> on page 1023.
Livelink	See <a href="#">“Setting up scanning of Livelink repositories”</a> on page 1033.
Web servers (Web sites and Web-based applications)	See <a href="#">“Setting up scanning of Web servers”</a> on page 1011.

**6** Configure optional Network Discover target parameters.

See [“Network Discover scan target configuration options”](#) on page 855.

## 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 850.

### To edit a Network Discover target

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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 855.



# 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 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**, and **Advanced** tabs to configure a Network Discover scan target.

The **General** tab is available for all types of targets.

The **Scanned Content** and **Advanced** tabs are only available for some types of targets.

See [“Editing an existing Network Discover target”](#) on page 852.

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 everything, 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. These required fields should be set when a new target is added.	General tab	See <a href="#">“Configuring the required fields for Network Discover targets”</a> on page 857.
Schedule Network Discover scans.	General tab	See <a href="#">“Scheduling Network Discover scans”</a> on page 858.
Configure incremental scans.	General tab	See <a href="#">“Scanning new or modified files (an incremental scan)”</a> on page 884.
Provide authentication, and set up credentials.	Scanned content tab	See <a href="#">“Providing the password authentication for Network Discover scanned content”</a> on page 860.
Include, or exclude, repositories from a scan.	Scanned content tab	See <a href="#">“Setting up Discover filters to include or exclude items from the scan”</a> on page 861.
Filter targets by file size.	Scanned content tab	See <a href="#">“Filtering Discover targets by item size”</a> on page 864.
Filter targets by date last accessed or modified.	Scanned content tab	See <a href="#">“Filtering Discover targets by date last accessed or modified”</a> on page 865.
Optimize your resources with scan throttling.	Advanced tab	See <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.
Create an inventory of the locations of unprotected sensitive data.	Advanced tab	See <a href="#">“Creating an inventory of the locations of unprotected sensitive data”</a> on page 869.

Optional tasks	Tab in scan target	Description of task
Move or quarantine files in network file shares with Network Protect.	Protect tab	See <a href="#">“Configuring Network Protect for file shares”</a> on page 906.

## 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

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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, enter the **Name** of this Discover target.  
Enter a unique name for the target, or edit the existing name, up to 255 characters.
- 4 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.

- 6 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 843.
- 7 You can configure other options for this target.  
See [“Network Discover scan target configuration options”](#) on page 855.

## 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 855.

### To set up a scan schedule

- 1 In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2 Click the name of the scan that you want to schedule.
- 3 Click the **General** tab.
- 4 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 Daily	Scan the target daily, at the specified start time. Check <b>Until</b> to stop the daily scan after a certain date.
Scan Weekly	Scan the target every week. Check <b>Until</b> to stop the weekly scan after a certain date.
Scan Monthly	Scan the target every month. Check <b>Until</b> to stop the monthly scan after a certain date.

**6** Click **Save**.

**To pause a scan during specified times**

- 1** In the Enforce Server administration console, on the **Manage** menu, click **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

- 1 In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2 Click the name of the scan to provide the password authentication.
- 3 Click the **Scanned Content** tab.
- 4 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 list.  
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 843.
- 6 You can set other options on the **Scanned Content** tab.  
See [“Network Discover scan target configuration options”](#) on page 855.  
Remediation credentials can be set on the **Protect** tab.  
See [“Configuring Network Protect for file shares”](#) on page 906.

## Encrypting passwords in configuration files

Encrypt passwords in the configuration files with the utility `EncryptPassword.exe`.

### To encrypt passwords in configuration files

- 1 Navigate to the `bin` directory of the scanner installation on the scanner computer.  
See [“Scanner installation directory structure”](#) on page 955.
- 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.
- 5 Place the encrypted password into the `Password=` setting in the `Vontusscanner_typeScanner.cfg` file.

See [“Configuration options for Exchange scanners”](#) on page 981.

See [“Configuration options for SharePoint 2003 scanners”](#) on page 1008.

See [“Configuration options for Web server scanners”](#) on page 1016.

See [“Configuration options for Documentum scanners”](#) on page 1028.

See [“Configuration options for Livelink scanners”](#) on page 1039.

## Setting up 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 880.

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.

When both include filters and exclude filters are present, exclude filters take precedence.

You can configure other options for this target.

See [“Network Discover scan target configuration options”](#) on page 855.

#### **To set up include filters or exclude filters**

- 1** In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2** Click the name of the scan where you want to add include filters or exclude filters.
- 3** Click the **Scanned Content** tab.

- 4 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 45-1 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**

- 1 Create a directory named `excludeFiles` in the Symantec Data Loss Prevention configuration directory, for example `\Vontu\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 *hostname* in this text file must match exactly the name that is in the Discover Target.
- 3 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 45-1 shows the syntax for the filters.

**Table 45-1** Syntax for the Include Filters and Exclude Filters

* (asterisk)	Use this wildcard to match any sequence of characters, including null.
? (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.

**Table 45-1** Syntax for the Include Filters and Exclude Filters (*continued*)

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.

The following example of an Include Filter matches only files or documents with the .txt or .doc extensions, ignoring everything else:

```
*.txt, *.doc
```

The following 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`:

```
*.?
```

You can also use filters to match on specific subdirectories of a file share. For example, to match only those files that are contained in the two subdirectories that are called `documentation` and `specs`, enter the following include filter:

```
*/documentation/*, */specs/*
```

Syntax and examples for SQL Database scanning are in the SQL Database section. See [“Configuring and running SQL database scans”](#) on page 920.

Syntax and examples for SharePoint scanning are in the SharePoint section. See [“Configuring and running SharePoint server scans”](#) on page 931.

Syntax and examples for Endpoint Discover scanning are in the Endpoint section. See [“How to implement Endpoint Discover”](#) on page 1067.

## 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 855.

#### To exclude items based on item size

- 1 In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2 Click the name of the scan that you want to filter based on item size.
- 3 Click the **Scanned Content** tab.
- 4 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.

- 5 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.
- 6 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 only available for files on file shares, Endpoint files, and Lotus Notes documents.

Incremental scanning and differential scanning are available for some Network Discover target types.

See [“Scanning new or modified files \(an incremental scan\)”](#) on page 884.

See [“Scanning new or modified items \(a differential scan\)”](#) on page 886.

You can configure other options for this target.

See [“Network Discover scan target configuration options”](#) on page 855.

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

- 1 In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2 Click the **Scanned Content** tab.
- 3 Enter optional values under **File Date Filters**.
- 4 Select **Only Scan files added or modified since the last full scan** for a differential scan.

See [“Scanning new or modified items \(a differential scan\)”](#) on page 886.

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 883.

See [“About the difference between incremental scans and differential scans”](#) on page 882.

- 5 Select **Only scan files added or modified** to include files based on the added 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.

**6** 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`.

---

- 7 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 880.

**To set scan throttling for file shares, Lotus Notes documents, or SQL Databases**

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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.
- 4 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**

- 1 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 Incidents By`.

- Lotus Notes databases

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 855.

#### To create an inventory of sensitive data

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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.



# Managing Network Discover target scans

This chapter includes the following topics:

- [Managing Network Discover target scans](#)
- [Network Discover scan target list](#)
- [Network Discover target scan status](#)
- [Network Discover scan detail](#)
- [Network Discover scan history](#)
- [About Network Discover scan optimization](#)
- [About the difference between incremental scans and differential scans](#)
- [About incremental scans](#)
- [Scanning new or modified files \(an incremental scan\)](#)
- [Managing incremental scans](#)
- [Scanning new or modified items \(a differential scan\)](#)
- [Configuring parallel scanning of Network Discover targets](#)
- [Removing Network Discover scan targets](#)
- [Deleting Network Discover scans](#)

## Managing Network Discover target scans

After a new target is configured, the scan must be started manually, unless it was set up as a scheduled scan.

Click the play icon to start a scan.

While the scan is running, and after it has completed, you can monitor the state of the scan. You can also view details about the scan and the incidents found.

Incident reports are also available.

See [“About incident reports for Network Discover”](#) on page 890.

### To monitor Network Discover target scans

- 1 In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Targets**.
- 2 The initial **Discover Targets** screen displays an overview of the status of all target scans.

See [“Network Discover scan target list”](#) on page 874.

Click the play icon to start a scan.

- 3 On the **Manage** menu, click **Discover Scanning > Discover Servers** to list the detection servers for Network Discover or Endpoint Discover that are configured on your network.

See [“Network Discover target scan status”](#) on page 875.

- 4 On the **Manage** menu, click **Discover Scanning > Discover Targets**, and then click **show all scans**. Click a particular scan to see the scan details.

See [“Network Discover scan detail”](#) on page 876.

- 5 On the **Manage** menu, click **Discover Scanning > Discover Targets**, and then click **show all scans** to see the history of a particular scan target. You can see the times when the scan ran.

- 6 See [“Network Discover scan history”](#) on page 879.

## Network Discover scan target list

The Discover Targets screen lists the target scans and summary status.

Additional information is available for monitoring Network Discover scans.

See [“Managing Network Discover target scans”](#) on page 874.

[Table 46-1](#) lists the columns for each target scan.

**Table 46-1** Discover Targets

Target Information	Description
<b>Target</b>	Name of the target scan.
<b>Scan</b>	Status (Ready, Paused, Running). If the scan is running, the detection server where the scan is running is displayed.  The icons are to start the scan (play icon), pause, or stop the scan.  Below this status line is a list of the completed scans. Click any of the scans to display the details for that scan.
<b>Run Time</b>	Run time for this scan.
<b>Scan Type</b>	Scan type, such as incremental, differential, or full.
<b>Items Scanned</b>	Total items scanned.
<b>Bytes Scanned</b>	Total bytes scanned.
<b>Errors</b>	Errors that occurred during the scan.
<b>Incidents</b>	The number of incidents that are found during this scan. Click the number of incidents for details about these incidents.
<b>Schedule</b>	Date and time when the scan is scheduled to start next, or scheduled to pause (if running).

## Network Discover target scan 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.

Icons appear at top right to return you to the screen you viewed last, or to refresh the current screen with the latest data.

Additional information is available for monitoring Network Discover scans.

See [“Managing Network Discover target scans”](#) on page 874.

[Table 46-2](#) lists the information for each server.

**Table 46-2** Discover Servers

Server Information	Description
Server Name	The name of the server. In parenthesis 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 queued scans, which, when removed from the queue, can run on this server.
Scheduled Scans	A list of scans (that are scheduled to run in the future) which may be run on this server when they run.
Paused Scans	A list of the paused scans that may run on this server when they are resumed.

## Network Discover scan detail

The Scan Detail screen displays details about the scan that last ran, or is currently running, on the target.

Additional information is available for monitoring Network Discover scans.

See [“Managing Network Discover target scans”](#) on page 874.

[Table 46-3](#) shows the General section which displays information about the scan.

**Table 46-3** General Scan Detail

General Scan Detail	Description
Target Type	The type and the icon of the target that was scanned.
Target Name	The name of the target.
Status	The 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 46-4](#) shows the Scan Statistics section, which provides detailed information about the scan.

**Table 46-4** Scan Statistics

Scan Statistics	Description
<b>Processed</b>	The number of items that were scanned is compared to the total number of items to scan. If the scan is still running, this field provides a benchmark of scan progress.
<b>Run Time</b> (dd:hh:mm:ss)	The amount of time, expressed in days (if needed), hours, minutes, and seconds, 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.
<b>Items Scanned</b>	The number of items scanned.
<b>Bytes Scanned</b>	The amount of disk space (in bytes) that was scanned.
<b>Errors</b>	The number of errors that occurred during the scan. A list of the errors is available in the Recent Scan Errors section.
<b>Incident Count</b>	The number of incidents that were detected during the scan. You can click on this number to see an Incident List for this scan.

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 46-5](#) shows the information in the Recent Scan Errors report, which provides information about each error.

**Table 46-5** Recent Scan Errors

Recent Scan Error Details	Description
Date	The date and time of the error during the scan.

**Table 46-5** Recent Scan Errors (*continued*)

Recent Scan Error Details	Description
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 46-6](#) shows the Recent Scan Activity report, which provides information about each activity.

**Table 46-6** Recent Scan Activity

Recent Scan Activity Details	Description
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 46-7](#) explains the options on the Scan Detail screen.

**Table 46-7** Options on the Scan Detail screen

Scan Detail options	Description
<b>Download Full Statistics Report</b>	Initiates the download of a report with all scan statistics.
<b>Download Full Error Report</b>	Initiates the download of a report with all scan errors.
<b>Download Full Activity Report</b>	Initiates the download of a report with all scan activity.
	Returns you to the screen you viewed last.
	Refreshes the current screen with the latest data.

# Network Discover scan history

The **Scan History** screen displays a list of all scans that were performed on the selected target.

Additional information is available for monitoring Network Discover scans.

See “[Managing Network Discover target scans](#)” on page 874.

[Table 46-8](#) lists the fields that are displayed for each scan.

**Table 46-8** Scan History

Scan History	Description
<b>Started</b>	Date and time the scan started.
<b>Finished</b>	Date and time the scan finished.
<b>Status</b>	Current status of the scan (Aborted, Completed, or Failed).
<b>Run Time</b> dd:hh:mm:ss	Amount of time (in days, hours, minutes, and seconds) that the scan has been running or ran.
<b>Scan Type</b>	Scan type, such as incremental or full.
<b>Items Scanned</b>	The number of items that were scanned in the target.
<b>Bytes Scanned</b>	Amount of disk space (in bytes) scanned in the target.
<b>Errors</b>	Number of errors during the scan.
Delete icon	Click the delete icon at the end of the row to delete this scan. Make sure to first delete all the incidents from that scan, and delete differential scans before you delete the base scan.  See “ <a href="#">Deleting Network Discover scans</a> ” on page 888.

You can click any column header to sort the list alpha-numerically by that column’s data.

Click a column header to sort in ascending order. Click it again to sort in descending order.

For more details about a scan, click on details to display the Scan Detail screen.

## About Network Discover scan optimization

First, focus on the file shares or repositories that are the most accessed and most widely available (for example, guest or public access). Start small, and confirm the accuracy before increasing the volume of information in a scan.

Next, target the business units that handle your confidential data.

To optimize your scans of large amounts of information, follow the suggestions in this section.

Network Discover Target scans can take hours or days to complete. The time depends on the type of scan, and the amount and format of the data to be scanned. It also depends on the hardware on the host computer, and the network speed.

Certain files take longer to scan than others. For example, PDFs, the documents that contain regular expressions, and the spreadsheets that contain formulas all take longer than average to scan.

To help optimize your Network Discover scans, consider using some of the following methods:

- 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 Discover filters to include or exclude items from the scan”](#) on page 861.  
See [“Filtering Discover targets by item size”](#) on page 864.  
See [“Filtering Discover targets by date last accessed or modified”](#) on page 865.
- 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 target.

See [“Setting up Discover filters to include or exclude items from the scan”](#) on page 861.

- 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 files \(an incremental scan\)”](#) on page 884.  
 See [“About the difference between incremental scans and differential scans”](#) on page 882.
- 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 865.
- 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 \(a differential scan\)”](#) on page 886.  
 See [“About the difference between incremental scans and differential scans”](#) on page 882.
- 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 864.
- 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 Discover filters to include or exclude items from the scan”](#) on page 861.
- 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 920.  
 Use the Include filter to scan spreadsheet files:  

```
*.xls
```

 Then set up a separate scan target and use the Exclude Filter to scan everything else.  
 See [“Setting up Discover filters to include or exclude items from the scan”](#) on page 861.

- 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 901.  
See [“Configuring and running scans of file shares”](#) on page 902.
- 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 869.
- Dedicate as much hardware as possible to the Symantec Data Loss Prevention scans. For example you can 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 886.
- Use throttling to reduce network load.  
See [“Optimizing resources with Network Discover scan throttling”](#) on page 868.
- Update the server hardware.  
You can use up to 12 GB of memory, quad CPUs, ultra-fast hard drives, and Endace network cards to address any bottlenecks in the hardware.

## About the difference between incremental scans and differential scans

To optimize scans, you can scan only the items that have not previously been scanned, or that have not been scanned before. You can accomplish this optimization with either incremental scans or differential scans. Depending on the target server type, either incremental scans or differential scans are available.

See [“About incremental scans”](#) on page 883.

See [“Scanning new or modified files \(an incremental scan\)”](#) on page 884.

See [“Scanning new or modified items \(a differential scan\)”](#) on page 886.

[Table 46-9](#) compares incremental scans versus differential scans.

**Table 46-9** Differences between incremental scans and differential scans

Incremental scans	Differential scans
<p>Incremental scans are supported for the following targets:</p> <ul style="list-style-type: none"> <li>■ <b>Server &gt; File System</b></li> </ul>	<p>Differential scans are supported for the following targets:</p> <ul style="list-style-type: none"> <li>■ <b>Server &gt; Lotus Notes</b></li> <li>■ <b>Server &gt; SharePoint</b></li> <li>■ <b>Server &gt; Exchange</b></li> <li>■ <b>Endpoint &gt; File System</b></li> </ul> <p>Some of the scanners have a configuration option that is similar to differential scanning. Refer to the configuration parameters for the individual scanner targets.</p>
<p>Partial scans retain the information about the items that have been scanned.</p> <p>If files, shares, or items are missed because they are inaccessible, the next incremental scan automatically covers the missed items.</p>	<p>Begin with a full scan of the Discover target. This full scan is called the base scan.</p> <p>Partial scans cannot be used as a base scan.</p>
<p>Subsequent runs scan all items that have not previously been scanned, including new or modified items.</p>	<p>Subsequent runs scan all items that have been added or modified since the date of the most recent full (base) scan completed.</p>
<p>An incremental scan index keeps track of which items have already been scanned.</p>	<p>The most recent complete base scan serves as the comparison for which items to scan, based on the date of the base scan.</p>

## About incremental scans

Incremental scans are a way to let you resume a scan from where you left off, and to optimize your scanning.

See [“About Network Discover scan optimization”](#) on page 880.

Incremental scanning is only supported for some targets types.

See [“About the difference between incremental scans and differential scans”](#) on page 882.

Incremental scans retain the information about the items that have been scanned.

Subsequent runs scan all items that have not previously been scanned. Subsequent scans include new or modified items, and the items that were missed from a previously incomplete scan.

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, for example 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*.

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*. The existing targets that are not configured for differential scanning are upgraded to be a full scan.

## Scanning new or modified files (an incremental scan)

An incremental scan lets you resume a Network Discover scan from where you left off. An incremental scan scans only the items that have not been scanned previously.

For some targets, scans can only be configured as differential. Targets can be configured for differential scanning or incremental scanning options, but not both.

See [“Scanning new or modified items \(a differential scan\)”](#) on page 886.

For a list of which target types support differential or incremental scanning, see the following topic.

See [“About the difference between incremental scans and differential scans”](#) on page 882.

### To set up an incremental scan

- 1 Click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the drop-down **New Target**, and select the **File System** target type, or select one of the file system scan targets in the list to edit it.
- 3 Click the **General** tab.

- 4 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 857.  
  
See [“Network Discover scan target configuration options”](#) on page 855.  
  
See [“Setting up scans of file shares”](#) on page 899.
- 6 To manage incremental scanning and diagnose issues, refer to the following topic:  
  
See [“Managing incremental scans”](#) on page 885.

## Managing incremental scans

While running incremental scans, observe the following items:

- 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 removed.

## Scanning new or modified items (a differential scan)

To save resources, scans can be differential, and only scan the items that are added or modified since the last full scan.

For some targets, scans can be incremental, and only scan the items that have not yet been scanned.

See [“Scanning new or modified files \(an incremental scan\)”](#) on page 884.

See [“About the difference between incremental scans and differential scans”](#) on page 882.

### To set up a differential scan

- 1 Click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the drop-down **New Target**, and select the target type, or select one of the scan targets in the list to edit it.
- 3 Click the **Scanned Content** tab.
- 4 Select the date option for a differential scan.  
See [“Filtering Discover targets by date last accessed or modified”](#) on page 865.
- 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 share with different credentials, and from the same Network Discover Server is not supported.

The scan can be controlled (paused, resumed, or aborted) 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 952.

#### To configure parallel scanning

- 1 In the Enforce Server administration console, on the **System** menu, click **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 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 on the Network Discover Server.

- 6 Click **Save**.
- 7 Click **Done**.
- 8 You can view the scans that are actively running, queued, scheduled, or paused on each Network Discover Server. In the Enforce Server administration console, on the **Manage** menu, click **Discover Scanning > Discover Servers**.

See [“Managing Network Discover target scans”](#) on page 874.

## Removing Network Discover scan targets

Monitor the scans that are running or queued before removing a scan target.

See [“Managing Network Discover target scans”](#) on page 874.

You can remove a scan target in any of the following ways:

- Remove the scan target from the Enforce Server.
- For scanners, uninstall the scanner from the computer where the scanner is installed.

#### To remove a scan target

- 1 From the Enforce Server administration console, click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the **X** that appears on the far right of the target you want to remove.

#### To remove a scanner on a Windows system

- 1 From the Enforce Server administration console, click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the **X** that appears on the far right of the target you want to remove.
- 3 On the system with the scanner, log on as Administrator and click the Windows **Start** icon.
- 4 Select **Programs > Vontu Scanner > scanner\_name > Uninstaller**.

#### To remove a scanner on a UNIX system

- 1 From the Enforce Server administration console, click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the **X** that appears on the far right of the target you want to remove.
- 3 On the system with the scanner, log on as root and type the following:

```
# /opt/scanner/uninstall
```

## Deleting Network Discover scans

You can delete a specific scan.

#### To delete a scan

- 1 Display the **Scan History** screen.  
See “[Network Discover scan history](#)” on page 879.
- 2 Delete all the incidents from that scan.
- 3 Delete any differential scans before you delete the base full scan for that target.  
This step is not necessary for incremental scans.
- 4 To delete the scan, locate the scan to be deleted, and click the delete icon at the end of the line.

# Managing Network Discover incident reports

This chapter includes the following topics:

- [About reports for Network Discover](#)
- [About incident reports for Network Discover](#)

## 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 the details confidential data that is exposed.

See [“About incident reports for Network Discover”](#) on page 890.

For information about Network Discover targets, scan details, and scan history, on the **Manage** menu, select **Discover Scanning > Discover Targets**. Then select one of the Discover targets from the list.

See [“Managing Network Discover target scans”](#) on page 874.

Information about Network Discover targets, scan details, and history can be viewed from the following screens:

- **Network Discover Targets**  
This report is on the Enforce Server administration console, **Manage** menu, **Discover Scanning > Discover Targets**.  
See [“Network Discover scan target list”](#) on page 874.
- **Scan Status**

This report is on the Enforce Server administration console, **Manage** menu, **Discover Scanning > Discover Servers**.

See [“Network Discover target scan status”](#) on page 875.

■ **Scan Details**

This report is from the Enforce Server administration console, **Manage** menu, **Discover Scanning > Discover Targets**. Click **show all scans**. Click a particular scan to see the scan details.

See [“Network Discover scan detail”](#) on page 876.

■ **Scan History**

This report is from the Enforce Server administration console, **Manage** menu, **Discover Scanning > Discover Targets**. Click **show all scans** to see the history of a particular scan target.

See [“Network Discover scan history”](#) on page 879.

## 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 745.

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 753.

See [“About filters and summary options for reports”](#) on page 761.

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**.

---

**Note:** Network Discover does not retain the original files that generated an incident. Access the files that generate incidents by clicking the link on the **Incident Snapshot** screen. The logon credentials of the user on the local computer where the browser is running determine the permission to open those files.

---



# Using FlexResponse custom plug-ins to remediate incidents

This chapter includes the following topics:

- [Using Server FlexResponse custom plug-ins to remediate incidents](#)
- [Creating Response Rules that use incident response actions](#)
- [Locating incidents for remediation](#)
- [Using the action of a Server FlexResponse plug-in to remediate an incident](#)
- [Verifying the results of a manual incident response action](#)

## Using Server FlexResponse custom plug-ins to remediate incidents

You can manually remediate Network Discover incidents with custom plug-ins.

To develop a custom remediation action, see the *Symantec Data Loss Prevention Server FlexResponse Platform Developers Guide*.

To manually remediate incidents with custom Server FlexResponse plug-ins, you must perform the following steps:

Table 48-1

Step	Action	Description
Step 1	Create a response rule which uses a custom Server FlexResponse incident response action.	See <a href="#">“Creating Response Rules that use incident response actions”</a> on page 894.
Step 2	Locate incidents for remediation.	See <a href="#">“Locating incidents for remediation”</a> on page 895.
Step 3	Use the action of the Server FlexResponse plug-in to remediate incidents.	See <a href="#">“Using the action of a Server FlexResponse plug-in to remediate an incident”</a> on page 896.
Step 4	Verify the results.	See <a href="#">“Verifying the results of a manual incident response action”</a> on page 897.

## Creating Response Rules that use incident response actions

Create a Network Protect Response Rule that uses your Server FlexResponse plug-in.

### To create a Network Protect Response Rule

- 1 Log on to the Enforce Server console.
- 2 Create a new Response Rule for each custom Server FlexResponse plug-in.  
Click **Policies > Response Rules**.
- 3 Click **Add Response Rule**.
- 4 Select **Smart Response**. Click **Next**.
- 5 Enter a name for your test rule. This name is the label on the button that can be selected in the display during remediation.
- 6 Enter an optional description for your test rule.
- 7 In the drop-down **choose action type** select the action **All: Server FlexResponse**.
- 8 Click **Add Action**.

- 9 In the drop-down **choose a plugin**, select the custom Server FlexResponse plug-in for this Response Rule.

The name that shows 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.

- 10 Click **Save**.
- 11 Repeat this procedure, adding a Response Rule for any additional Server FlexResponse plug-ins.

## Locating incidents for remediation

Use the reports on the Enforce Server to select incidents for remediation.

### To locate incidents for remediation

- 1 Log on to the Enforce Server 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.
- 4 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.
- 5 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”](#) on page 896.

# Using the action of a Server FlexResponse plug-in to remediate an incident

After you have selected an incident, or group of incidents to remediate, you can invoke the action. This action uses your custom Server FlexResponse plug-in to remediate the incidents manually.

## To remediate a single incident

- 1 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 remediation”](#) on page 895.

- 3 In the **Incident Detail** screen above the incident number, your remediation options display. These options show the names of your Response Rules.

- 4 Click a Server FlexResponse plug-in remediation button to perform the remediation action.

- 5 View the remediation action. Click **OK**.

- 6 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 a manual incident response action”](#) on page 897.

## To remediate a selected group of incidents

- 1 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 remediation”](#) on page 895.

- 2 **Incident Actions** becomes a drop-down list.

- 3 From the **Incident Actions** drop-down, select **Run Smart Response** and then select your custom Server FlexResponse.

- 4 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 a manual incident response action”](#) on page 897.

## Verifying the results of a manual incident response action

After you complete the manual remediation of incidents, you can verify that the remediation action has been completed.

### To verify the results of a manual incident response action for a single incident

- 1 Log on to the Enforce Server console.
- 2 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**.
- 4 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 a manual incident response action for a group of incidents

- 1 Log on to the Enforce Server console.
- 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 786.

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 753.



# Setting up scans of file shares

This chapter includes the following topics:

- [Setting up scans of file shares](#)
- [Supported file share targets](#)
- [Excluding internal DFS folders](#)
- [Configuring scans of Microsoft Outlook Personal Folders \(.pst files\)](#)
- [Configuring and running scans of file shares](#)
- [Configuring Network Protect for file shares](#)

## Setting up scans of file shares

Network Discover scans network shares (CIFS, NFS, DFS, or any other client) to discover confidential data. Network Discover can also scan Microsoft Outlook Personal Folders (.pst files) on network file shares.

To set up scanning of file shares, complete the following process:

**Table 49-1**      Setting up a network file share scan

Step	Action	Description
Step 1	Verify that your network file share is on the list of supported targets.	See <a href="#">“Supported file share targets”</a> on page 900.

**Table 49-1** Setting up a network file share scan (*continued*)

Step	Action	Description
Step 2	Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create a new target for a file share and to configure scanning of file shares.	See <a href="#">“Configuring and running scans of file shares”</a> on page 902.
Step 3	Set any additional scan target configuration options.  For scanning of Microsoft Outlook Personal Folders, verify that the option is set.	See <a href="#">“Network Discover scan target configuration options”</a> on page 855.  See <a href="#">“Configuring scans of Microsoft Outlook Personal Folders (.pst files)”</a> on page 901.
Step 4	To automatically move or quarantine files, configure Network Protect.	See <a href="#">“Configuring Network Protect for file shares”</a> on page 906.
Step 5	Start the file share scan.  Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> .	Click the Play icon for the scan target on this list.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Managing Network Discover target scans”</a> on page 874.

## Supported file share targets

The File Systems (Server) target supports scanning of the following network file shares:

- CIFS on Windows
- NFS on Linux
- DFS scanning on Windows 2003 and Windows 2008. DFS is not supported with Network Protect.

In addition, the File Systems (Server) target supports scanning of the following file types:

- Microsoft Outlook Personal Folders (.pst files) created with Outlook 1997-2002, 2003, and 2007.

The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2003 SP3 or later must be installed there. See [“Configuring scans of Microsoft Outlook Personal Folders \(.pst files\)”](#) on page 901.

- File systems on UNIX systems can also be scanned, 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. Contact Symantec Professional Services for details.

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`.

## Excluding internal DFS folders

By default, DFS file share scans scan the dynamic internal DFS folders that DFS creates. These folders are internal to DFS, so they do not need to be scanned.

### To exclude DFS internal folders

- 1 In the Enforce Server administration console, click **Manage > Discover Scanning > Discover Targets**.
- 2 Click the name of the scan where you want to add the exclude filter for the DFS internal folders.
- 3 Click the **Scanned Content** tab.
- 4 Enter `/DfsrPrivate/*` in the **Exclude Filters** field.
- 5 Click **Save**.

## Configuring scans of Microsoft Outlook Personal Folders (.pst files)

Microsoft Outlook Personal Folders (.pst files) can be scanned by selecting the option **Scan PST Files** on the **Advanced** tab.

Microsoft Outlook Personal Folders (.pst files) can be scanned on file shares. The scan supports Microsoft Outlook Personal Folders (.pst files) that were created with Outlook 1997-2002, 2003, and 2007.

See [“Configuring and running scans of file shares”](#) on page 902.

The following notes pertain to scanning .pst files:

- The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2003 SP3 or later must be installed there. If your Network Discover Server for the scan is running 32-bit Windows, then 32-bit Outlook must be installed. If your Network Discover Server for the scan is running 64-bit Windows, then 64-bit Outlook must be installed.
- 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

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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 shares”](#) on page 902.
- 3 On the **Advanced** tab, check the box **Scan PST files**. This setting is the default.

## Configuring and running scans of file shares

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 file shares

- 1 In the Enforce Server administration console, on the **Manage** menu, click **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, enter the **Name** of this Discover target.  
Enter a unique name for the target, or edit the existing name, up to 255 characters.

**4 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.

**6 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)**

**7 On the **Scanned Content** tab, enter the credentials (default and overriding).**

You can specify a default user name to use for access to all file shares, except those specified using the **Add** editor.

The password must not contain the quotation mark character. If any of your passwords contain a quotation mark character, those shares 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`.

**8 Under **Shares**, enter the item to be scanned.**

Select one of the following methods of entering the file shares:

- Scan shares from an uploaded file

Create and save a plain text file (.txt) listing the servers you want to scan. Then click **Browse** to locate the list and **Upload Now** to import it. Create a file using an ASCII text editor and enter one file 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.

```
\\share\marketing  
nfs:\\share\marketing  
//share/engineering/documentation  
/home/protect/mnt/server/share/marketing  
c:\share\engineering
```

#### ■ Scan individual shares

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.

```
[\\hostname\path,username,password,depth,username2,password2]
```

### 9 Select Path Filters.

Use the Include Filter and Exclude Filter 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 Filter, 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 Discover filters to include or exclude items from the scan”](#) on page 861.

When scanning DFS shares, exclude the internal DFS folder.

See [“Excluding internal DFS folders”](#) on page 901.

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`.

### 10 Select 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 Select 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 this field empty, Symantec Data Loss Prevention performs matching on files or documents of all sizes.

## 12 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.

## 13 Select the **Advanced** tab for options to optimize scanning. On the **Advanced** tab, you can configure throttling options, set Inventory Mode for scanning, and omit or select scanning of Outlook `.pst` files.

### ■ Throttling Options

Specify the maximum number of files 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 moving on to the next item to scan (a file share 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 item to scan, rather than scanning everything.

After the incident threshold has been reached, the scanning of this item is stopped, and scanning proceeds to the next item. Because the process is asynchronous, a few more incidents may be created than specified in the incident threshold.

Select **Content Root** (the default), or **Machine**.

The 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.

Select the **Machine** option to count by physical computer (from the specified shares on a 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.

Note that the physical computer name must be literally the same, for the item 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.

#### ■ PST Scanning

Check the **Scan PST Files** box to configure scanning of Outlook personal folders (`.pst` files).

The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2003 SP3 or later must be installed there.

See [“Configuring the required fields for Network Discover targets”](#) on page 857.

Clear the **Scan PST Files** box to scan as a regular file.

## 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 in the license, 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

- 1 Create a policy with a response rule. Go to **Manage > Policies > Response Rules** and click **Add Response Rule**.  
See [“About response rules”](#) on page 680.
- 2 Select **Automated Response**. Click **Next**.

- 3 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. Enter 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 quarantined 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.

Click **Save**.

- 4 Add a new policy, or edit an existing policy.  
See [“Configuring policies”](#) on page 338.
- 5 Click the **Response** tab, and in the pull-down menu, select one of the response rules that you previously created. 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.
- 6 Create a new file system Network Discover target, or edit an existing target.  
See [“Configuring and running scans of file shares”](#) on page 902.
- 7 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 quarantined (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.

- 8 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.

- 9 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 quarantine location and the original file's location. Specify the path (location) where the files are copied or quarantined. Enter 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 scans of Lotus Notes databases](#)
- [Supported Lotus Notes targets](#)
- [Configuring and running Lotus Notes scans](#)
- [Configuring Lotus Notes native mode configuration scan options](#)
- [Configuring Lotus Notes DIIOP mode configuration scan options](#)

## Setting up scans of Lotus Notes databases

You can configure scans of Lotus Notes repositories.

See [“Configuring and running Lotus Notes scans”](#) on page 911.

To set up scanning of Lotus Notes databases, complete the following process:

**Table 50-1**      Setting up a Lotus Notes database scan

Step	Action	Description
Step 1	Verify that your Lotus Notes database is on the list of supported targets.	See <a href="#">“Supported Lotus Notes targets”</a> on page 910.

**Table 50-1**      Setting up a Lotus Notes database scan (*continued*)

Step	Action	Description
Step 2	Configure the scan for Lotus Notes Native or DIIOP mode.	See “ <a href="#">Configuring Lotus Notes native mode configuration scan options</a> ” on page 913.  See “ <a href="#">Configuring Lotus Notes DIIOP mode configuration scan options</a> ” on page 916.
Step 3	Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create a Lotus Notes target and to configure scans of Lotus Notes databases.	See “ <a href="#">Configuring and running Lotus Notes scans</a> ” on page 911.
Step 4	Set any additional scan options for the Lotus Notes target.	See “ <a href="#">Network Discover scan target configuration options</a> ” on page 855.
Step 5	Start the Lotus Notes database scan.  Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> .	Click the Play icon for the scan target on this list.
Step 6	Verify that the scan is running successfully.	See “ <a href="#">Managing Network Discover target scans</a> ” on page 874.

## Supported Lotus Notes targets

The Lotus Notes target supports scanning of the following versions:

- Lotus Notes 7
- Lotus Notes 8
- Lotus Notes 8.5

The DIIOP configuration option is supported with both Windows and Linux Network Discover servers.

On Network Discover 32-bit servers, the native configuration is recommended, and a Lotus Notes client must be installed on the Network Discover Server. The DIIOP configuration option is supported with 64-bit Windows Servers. However, the native configuration option is supported only on 32-bit Network Discover

Windows Servers with a 32-bit Lotus Notes client installed on the Network Discover Server.

Lotus Notes 8.5 scan targets are supported with Linux 32-bit Network Discover Servers. You may need to add the following line in the protect user's `.bash_profile` and then restart the Vontu Monitor service:

```
LD_LIBRARY_PATH=  
$LD_LIBRARY_PATH:/opt/ibm/lotus/notes/data:/opt/ibm/lotus/notes
```

The files `Notes.jar` and `NCSO.jar` are in the Lotus Notes client installation directory. The `NCSO.jar` file is required only for DIIOP mode. 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

- 1 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 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 Discover filters to include or exclude items from the scan”](#) on page 861.

## 3 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 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.

## 5 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 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.

## 7 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.

## 8 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 869.

# Configuring Lotus Notes native mode configuration scan options

In the file `Crawler.properties`, when `lotusnotescrawler.use.diiop` is set to false, the Network Discover Server accesses the Domino server directly through a local Lotus Notes client. This mode is called "native." A Lotus Notes client must be installed on the Network Discover Server. Native mode is recommended from a standpoint of performance and security.

Lotus Notes scan targets can also be configured to scan in DIIOP mode. In DIIOP mode, no local client is required.

See [“Configuring Lotus Notes DIIOP mode configuration scan options”](#) on page 916.

### To configure a Lotus Notes native mode configuration for scanning

- 1 Copy only the Lotus Notes Java library file `Notes.jar` to the `Vontu_installation_directory\Protect\plugins` directory.

This file can be found in the installation directory of a Lotus Notes client installation.

This JAR file is in the following location in a Lotus Notes 8 client default installation:

```
C:\Program Files\IBM\lotus\notes\jvm\lib\ext\Notes.jar
```

This JAR file is in the following location in a Lotus Notes 7 client default installation:

```
C:\Program Files\lotus\notes\jvm\lib\ext\Notes.jar
```

This JAR file is in the following location in a Lotus Notes 6.5 client default installation:

```
C:\Program Files\lotus\notes\Notes.jar
```

Use the version of the `Notes.jar` file corresponding to the version of the Lotus Notes client.

See [“Supported Lotus Notes targets”](#) on page 910.

- 2 Edit the file `Vontu_installation_directory\Protect\config\Crawler.properties`.

Set the following property to `false`:

```
lotusnotescrawler.use.diiop = false
```

- 3 Install the Lotus Notes client on the Network Discover Server.

- 4 Give the Symantec Data Loss Prevention service user write permissions to the `notes.ini` file in the main Lotus Notes installation directory.

By default the Symantec Data Loss Prevention service user name is `protect`.

To change the permissions of this file on the Lotus Notes client, right-click the file `c:\Program Files\lotus\notes\notes.ini`. Select the **Properties** option. Select the **Security** tab. In the **Group or user names** section, select or add the `protect` user. In the permissions section, select the **Write** check box in the **Allow** column. Click **OK**.

- 5 Add the Lotus Notes home directory (for example `c:\Program Files\lotus\notes`) to the system `PATH` system variable.

Click **Start > Control Panel**. Double-click **System**. In the **System Properties** window, click the **Advanced** tab, and click **Environment Variables**. Edit the variable `PATH` and add a semicolon and the Lotus Notes path for example `c:\Program Files\lotus\notes` at the end of the variable value. Click **OK** to close each of the dialog boxes.

- 6 Copy the `user.id` user credential file (token) for the user performing the scan into the Lotus Notes directory `Program Files\lotus\notes\` of the client installation on the Network Discover Server. In the `user.id` file name, the `user` is the actual user name.

The permissions that are granted to this file determine the access to the Lotus Notes Domino server and the success of scanning operations. The Lotus Notes administrator must ensure that the `user.id` has the proper permissions to access all databases to scan.

- 7 Set up the user to perform the scan as the default user for the locally installed Lotus Notes client (through the Lotus Notes client user interface). There must be a `user.id` user credential file (token) for the user performing the scan in the `Program Files\lotus\notes\data` directory of the client installation. (This path is specified in the `notes.ini` file.) During a scan, the user name that is specified in the target configuration is ignored and the password is used to authenticate this default user.

- 8 Restart the Network Discover Server.

Click the Enforce Server **System** menu. Click the Network Discover Server for the **Server Detail**. Click **Recycle** to restart the Network Discover Server.

# 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.

Lotus Notes scan targets can also be configured to scan in native mode. Native mode is recommended from a standpoint of performance and security.

See [“Configuring Lotus Notes native mode configuration scan options”](#) on page 913.

## To configure a Lotus Notes DIIOP mode configuration for scanning

- 1 Copy the Lotus Notes Java library files `Notes.jar` and `NCSO.jar` to the `Vontu_installation_directory/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 910.

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 `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.
- 6 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 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 scans of SQL databases

You can configure scanning of Oracle, SQL Server, or DB2 databases.

See [“Configuring and running SQL database scans”](#) on page 920.

To set up scanning of SQL databases, complete the following process:

**Table 51-1**      Setting up a SQL database scan

Step	Action	Description
Step 1	Verify that your SQL database is on the list of supported targets.	See <a href="#">“Supported SQL database targets”</a> on page 920.

**Table 51-1** Setting up a SQL database scan (*continued*)

Step	Action	Description
Step 2	Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create a SQL database target and to configure scans of SQL databases.	See <a href="#">“Configuring and running SQL database scans”</a> on page 920.
Step 3	Set any additional scan options for the SQL database target.	See <a href="#">“Network Discover scan target configuration options”</a> on page 855.
Step 4	Install the JDBC driver for the SQL database, if needed.	See <a href="#">“Installing the JDBC driver for SQL database targets”</a> on page 923.
Step 5	Start the SQL database scan.  Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> .	Click the Play icon for the scan target on this list.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Managing Network Discover target scans”</a> on page 874.

## 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

#### 1 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, under the **Scanned Content**, 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=myinstance
```

##### ■ 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 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
```

### 3 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.

### 4 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 869.

## 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

#### 1 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 jTDS, 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.
- 4 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 924.

## 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 923.

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 query 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 query 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 scans of SharePoint servers](#)
- [About scans of SharePoint servers](#)
- [Supported SharePoint server targets](#)
- [Access privileges for SharePoint 2007 and 2010 scans](#)
- [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 scans of SharePoint servers

To set up scanning of SharePoint servers, complete the following process:

**Table 52-1**      Setting up a SharePoint server scan

Step	Action	Description
Step 1	Verify that your SharePoint server is on the list of supported targets.	See <a href="#">“Supported SharePoint server targets”</a> on page 930.

**Table 52-1**      Setting up a SharePoint server scan (*continued*)

Step	Action	Description
Step 2	<p>Verify that you have sufficient permissions to install the SharePoint solution on the Web Front Ends in a Farm.</p> <p>Also verify that the scan user has the permissions to run the scan of the SharePoint server.</p>	<p>See <a href="#">“Access privileges for SharePoint 2007 and 2010 scans”</a> on page 930.</p> <p>See <a href="#">“Installing the SharePoint solution on the Web Front Ends in a Farm”</a> on page 934.</p> <p>See <a href="#">“Configuring and running SharePoint server scans”</a> on page 931.</p>
Step 3	<p>Install the SharePoint solution on the Web Front Ends in a Farm.</p>	<p>See <a href="#">“Installing the SharePoint solution on the Web Front Ends in a Farm”</a> on page 934.</p>
Step 4	<p>Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create a SharePoint target and to configure scans of SharePoint servers.</p>	<p>See <a href="#">“Configuring and running SharePoint server scans”</a> on page 931.</p>
Step 5	<p>Set any additional scan options for the SharePoint target.</p>	<p>See <a href="#">“Network Discover scan target configuration options”</a> on page 855.</p>
Step 6	<p>Start the SharePoint server scan.</p>	<p>Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b>.</p> <p>Click the Play icon for the scan target on this list.</p>
Step 7	<p>Verify that the scan is running successfully.</p>	<p>See <a href="#">“Managing Network Discover target scans”</a> on page 874.</p>

## 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.

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 174.

See [“Importing SSL certificates to Enforce or Discover servers”](#) on page 168.

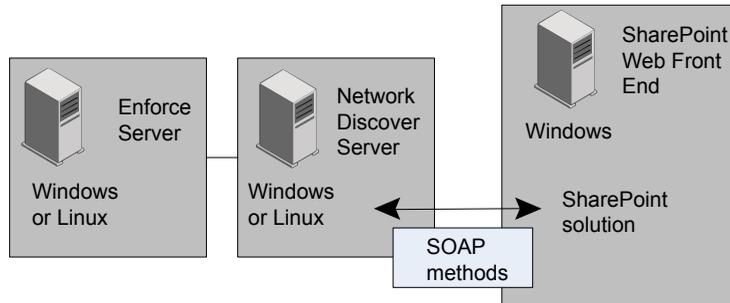
If the specified SharePoint site is configured to be on a port that is not the default (80), ensure that the SharePoint server allows the Discover Server to communicate on the required port.

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 931.

**Figure 52-1** 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
- Microsoft Office SharePoint Server 2007, on Windows Server 2003, 64-bit, or Windows 2008 R1
- Microsoft Office SharePoint Server 2010, on Windows Server 2008, 64-bit

SharePoint 2003 is supported only with the SharePoint scanner.

See [“Supported SharePoint scanner targets”](#) on page 993.

## Access privileges for SharePoint 2007 and 2010 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)

## 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 934.

**To set up a new target for the scan of a SharePoint server**

- 1 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 858.

**6** 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 2007 and 2010 scans](#)" on page 930.

**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 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, sub site, 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 Discover filters to include or exclude items from the scan”](#) on page 861.

## 9 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 865.

## 10 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 864.

**11** 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.

**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).

---

**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 2007 and 2010 scans”](#) on page 930.

### To install the Symantec SharePoint solution

**1** Copy the SharePoint solution installer `Symantec_DLP_Solution.exe` to a temporary directory on the SharePoint Web Front End. This file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Third_Party\SharePoint` or `DLPDownloadHome/Symantec_DLP_11_Lin/Third_Party/SharePoint` directory, where `DLPDownloadHome` is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

**2** Start the Windows SharePoint Services Administration service on the SharePoint server. On the SharePoint server, click **Start > All Programs > Administrative Tools > SharePoint Central Administration**.

**3** Double-click the `Symantec_DLP_Solution.exe` file. The Symantec Data Loss Prevention solution installation program starts.

**4** 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**.

**6** 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.

**8** Connect to **SharePoint Central Administration**. On the SharePoint server, click **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

- 1 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:\Vontu\Protect\config` (in a Windows default Symantec Data Loss Prevention installation).  
See [“Creating the configuration file for Active Directory integration”](#) on page 93.
- 2 Copy this file to the Discover Server into the folder `C:/Vontu/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 93.

- 4 On the Discover Server, update the `Protect.properties` file in the folder `C:\Vontu\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:/Vontu/jre/lib/security/krb5.ini
```

## Troubleshooting SharePoint scans

[Table 52-2](#) provides suggestions for troubleshooting issues with SharePoint scans.

**Table 52-2** 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.

**Table 52-2** Troubleshooting SharePoint scans (*continued*)

Issue	Recommended steps
No site collections, or only the default site collection, are scanned when the Discover Server and SharePoint site are in different domains.	<p>Specify the site collection/site/web application URL with a fully qualified domain name.</p> <p>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.</p> <p>Only the default site collection is scanned if the web application URL does not contain fully qualified domain name.</p>
The bytes reported as scanned does not match the number of bytes in the content.	<p>To improve performance, the scan statistics do not include items in the folders that are skipped (filtered out).</p> <p>Dynamic content, such as .aspx files, can change size.</p> <p>You can set the Advanced Server setting <code>Discover.countAllFilteredItems</code> to get more accurate scan statistics.</p> <p>See “<a href="#">Advanced server settings</a>” on page 174.</p>

# Setting up scans of Exchange servers

This chapter includes the following topics:

- [Setting up scans of Exchange repositories](#)
- [About scans of Exchange servers](#)
- [Supported Exchange server targets](#)
- [Providing access rights to scan all mailboxes and public folders](#)
- [Configuring and running Exchange server scans](#)
- [Example configurations and use cases](#)
- [Troubleshooting Exchange scans](#)

## Setting up scans of Exchange repositories

To set up scanning of Exchange servers, complete the following process:

**Table 53-1**      Setting up an Exchange server scan

Step	Action	Description
Step 1	Verify that your Exchange server is on the list of supported targets.	See <a href="#">“Supported Exchange server targets”</a> on page 941.
Step 2	Verify that your Exchange server provides Outlook Web Access. Also, WebDAV must be enabled.	

**Table 53-1** Setting up an Exchange server scan (*continued*)

Step	Action	Description
Step 3	If you need secure access between the Discover Server and your Exchange server or LDAP server, set up HTTPS and LDAPS.	See <a href="#">“Configuring and running Exchange server scans”</a> on page 943.
Step 4	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 <a href="#">“Providing access rights to scan all mailboxes and public folders”</a> on page 942.
Step 5	Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> to create an Exchange target and to configure scans of Exchange servers.	See <a href="#">“Configuring and running Exchange server scans”</a> on page 943.
Step 6	Set any additional scan options for the Exchange target.	See <a href="#">“Network Discover scan target configuration options”</a> on page 855.
Step 7	Start the Exchange server scan.	Click <b>Manage &gt; Discover Scanning &gt; Discover Targets</b> .  Click the Play icon for the scan target on this list.
Step 8	Verify that the scan is running successfully.	See <a href="#">“Managing Network Discover target scans”</a> on page 874.

## About scans of Exchange 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.

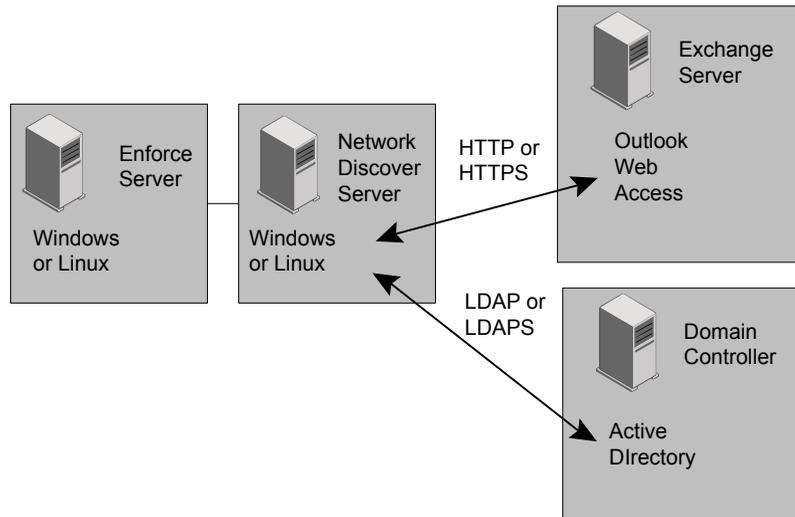
Communication is secure when the Exchange server is configured to use SSL (HTTPS). Communication to the LDAP server is secure when it is configured to use LDAPS.

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 174.

See “[Importing SSL certificates to Enforce or Discover servers](#)” on page 168.

**Figure 53-1** Exchange scan configuration



## Supported Exchange server targets

The following Exchange server targets are supported:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007

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 the Public Folders, for example the following data objects:

- Email messages
- Message attachments

- Microsoft Word documents
- Excel spreadsheets

The Exchange scan does not, however, target the mail that is stored in Personal Folders (.pst files) or offline folders (.ost files) that are not on the Exchange server. For scanning of .pst files on a file share, use the shared file system target.

See [“Configuring scans of Microsoft Outlook Personal Folders \(.pst files\)”](#) on page 901.

## 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, NTLM, 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

- 1 In the Exchange console, run the following to enable access to all mailboxes:

```
Get-Mailbox | Add-MailboxPermission -User specific_user -Accessright Fullac
```

- 2 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.

---

### For Exchange 2003, set up access rights to all mailboxes and public folders

- 1 Open the Exchange Server Manager.
- 2 Select **Servers** > *server\_name*, and make sure that access rights for the specific user are allowed. Look under the **Security** tab in the **Properties** dialog box for each Mailbox store and Public Folder store. Usually, all access rights are granted except **Receive As** and **Send As**.

- 3 Add the **Receive As** and **Send As** access rights.
- 4 Restart the Microsoft Exchange Information Store service to propagate the changes.

---

**Note:** The changes propagate automatically, but may take 15 minutes or longer.

---

## Configuring and running Exchange 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 168.

---

**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

- 1 Click **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 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 858.

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*

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 860.

7 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**

If a directory server is available, then select the **Directory Server** from the drop-down list.

To use this option, a connection to a Directory Server must be established. If no connection is set up, click the link **Create new Directory Connection** to jump to the page to configure the directory connection.

See "[Creating and managing directory server connections](#)" on page 513.

■ **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 "[Creating or modifying a User Group](#)" on page 517.

- **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**.

## 8 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 SharePoint 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 Discover filters to include or exclude items from the scan”](#) on page 861.

## 9 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 865.

## 10 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 864.

## 11 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.

## 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

[Table 53-2](#) lists the options to select on the **Scanned Content** tab during the configuration of an Exchange target.

**Table 53-2** Exchange scan use cases

Use case	Description
Scan all user mailboxes and public folders.	<p>Select the following options in the user interface:</p> <ul style="list-style-type: none"> <li>■ <b>All users on Directory Server</b></li> <li>■ <b>Public folders</b></li> </ul> <p>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).</p> <p>See <a href="#">“Providing access rights to scan all mailboxes and public folders”</a> on page 942.</p>
Scan all users mailboxes (but not public folders).	<p>Select the option <b>All users on Directory Server</b> in the user interface.</p> <p>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).</p> <p>See <a href="#">“Providing access rights to scan all mailboxes and public folders”</a> on page 942.</p>
Scan all public folders.	<p>Select the <b>Public folders</b> option in the user interface.</p> <p>The credentials must include a user who has access to the public folders.</p>
Scan all user mailboxes belonging to a specified group.	<p>Select the <b>Directory groups and users</b> option in the user interface.</p> <p>Then select the Directory Group from the groups in the list. All user mailboxes in the group are scanned.</p> <p>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).</p> <p>See <a href="#">“Providing access rights to scan all mailboxes and public folders”</a> on page 942.</p>
Scan an individual user mailbox.	<p>Select the <b>Directory groups and users</b> option in the user interface.</p> <p>Then enter the individual user mailbox name.</p> <p>The credentials must include access for the specified user mailbox.</p>

**Table 53-2** Exchange scan use cases (*continued*)

Use case	Description
Scan the user mailboxes that are not on the default store for Exchange.	<p>On the Exchange server, the user mailboxes may be in a different store than the default.</p> <p>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.</p>
Scan the public folders that are not on the default store for Exchange.	<p>On the Exchange server, the public folders may be in a different store than the default.</p> <p>Specify the Exchange URL containing the path to the public folders and credentials with access to the public folders.</p> <p>Select the <b>Public folders</b> option in the user interface.</p>

## Troubleshooting Exchange scans

[Table 53-3](#) provides suggestions for troubleshooting issues with Exchange scans.

**Table 53-3** Troubleshooting Exchange scans

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 number of bytes in the content.	<p>To improve performance, the scan statistics do not include items in the folders that are skipped (filtered out).</p> <p>You can set <code>Discover.countAllFilteredItems</code> in <b>Server Detail &gt; Advanced Server Settings</b> to get more accurate scan statistics.</p> <p>See "<a href="#">Advanced server settings</a>" on page 174.</p>

**Table 53-3** Troubleshooting Exchange scans (*continued*)

Issue	Recommended steps
<p>The connection to the Exchange server times out, and no items are scanned.</p>	<p>The default value for the timeout of the connection to the Exchange server is five minutes (300000 milliseconds).</p> <p>To increase the value, add and set the property in the configuration file <code>crawler.properties</code>. For example, to set the timeout to 10 minutes, add or modify the following line:</p> <pre>crawler.exchange.serverTimeout = 600000</pre>
<p>All items trigger incidents if the file type detection rule is set to detect Outlook Express items in the policy for an Exchange scan.</p>	<p>Remove Outlook Express from the file type detection rule.</p>

# About Network Discover scanners

This chapter includes the following topics:

- [How Network Discover scanners work](#)
- [Troubleshooting scanners](#)
- [Scanner processes](#)
- [Scanner installation directory structure](#)
- [Scanner configuration files](#)
- [Scanner controller configuration options](#)

## 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, [Figure 54-1](#) shows a two-tier configuration. This configuration has an Enforce Server and a Network Discover Server that is connected to a SharePoint server with a scanner installed.

You can perform the following tasks on the computers in this configuration:

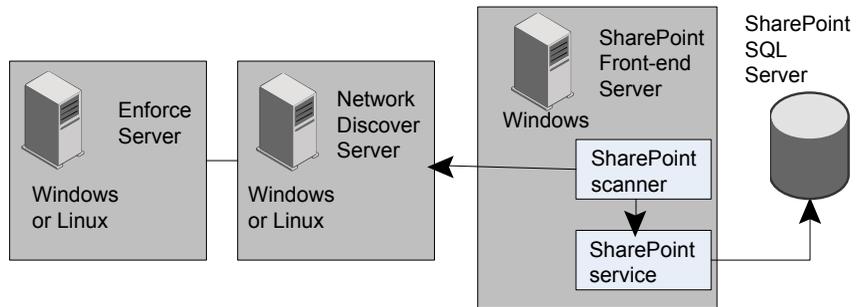
- On the Enforce Server, define the scan target (in this example, SharePoint).
- On the SharePoint server, install the SharePoint scanner, configure the scanner to post content to the Network Discover Server, and start (or stop) a scanner.
- On the Enforce Server, start or stop a target scan (with the Play 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.

**Figure 54-1** Example SharePoint scanner configuration



See “[About Network Discover](#)” on page 843.

## 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 951.

If a scanner does not seem to be processing items, use the following suggestions:

**Table 54-1** Scanner troubleshooting suggestions

Issue	Suggestions
Scanner does not seem to be running.	<p>Verify that the scanner was installed properly. Each scanner has its own installer.</p> <p>On the system where the scanner is installed, make sure that the scanner processes are running.</p> <p>See “<a href="#">Scanner processes</a>” on page 955.</p>

**Table 54-1** Scanner troubleshooting suggestions (*continued*)

Issue	Suggestions
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.
The scan does not seem to start.	Look in the <code>outgoing</code> folder.  See <a href="#">“Scanner installation directory structure”</a> on page 955.  If a given scanner cannot send content to Network Discover, that content queues up in the <code>outgoing</code> folder.  Items that appear and disappear from this folder indicate normal progress.

**Table 54-1** Scanner troubleshooting suggestions (*continued*)

Issue	Suggestions
<p>The scan appears stalled.</p>	<p>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.</p> <p>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.</p> <p>Verify that scan information moves through the scan process by checking the logs and temporary directories.</p> <p>See <a href="#">“Scanner installation directory structure”</a> on page 955.</p> <p>If the scan appears stalled, check the following locations on the scanner computer to diagnose the problem:</p> <ul style="list-style-type: none"> <li>■ The <code>/logs</code> folder           <p>The <code>/scanner_typeScanner/logs</code> 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.</p> </li> <li>■ The <code>/failed</code> folder           <p>Items that appear in the <code>/failed</code> 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 <code>/failed</code> folder.</p> </li> <li>■ The <code>/outgoing</code> folder           <p>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.</p> <p>If a given scanner cannot send content to Network Discover, that content queues up in the <code>/outgoing</code> folder.</p> </li> <li>■ The <code>/scanner_typeScanner/scanner</code> directory has the scanner connection status to the repository, repository crawling information, and fetched data.</li> </ul>

## Scanner processes

[Table 54-2](#) provides the information about Network Discover scanner processes on a Windows operating system.

**Table 54-2** Discover processes

Processes	Executable	Description
ScannerController	<i>scanner_typeScanner_Console.exe</i> or <i>scanner_typeScanner_Service.exe</i>	Process that configures and controls the connector, sends content to the Network Discover Server, and sends end-of-scan message to Network Discover.
Connector	<i>scanner_typeScanner.exe</i>	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 <code>KeyView</code> 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 54-3](#) describes the directory structure for Network Discover scanner configuration files.

**Table 54-3** Installation directory structure

Path	Description
<code>/scanner_typeScanner</code>	
<code>.../bin</code>	Files to run the scanner, start, and stop it.
<code>...../Clean.exe</code>	Cleans all temp files and logs under the <code>/scanner</code> directory.
<code>...../EncryptPassword.exe</code>	Can be used to encrypt the user names and passwords that are put in the <code>scanner_typeScanner.cfg</code> file.
<code>...../scanner_typeScanner_Console.exe</code>	Launches the scanner as a console application (with a window). Type CTRL+C to stop the scanner.
<code>...../scanner_typeScanner_Service.exe</code>	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.
<code>.../config</code>	Configuration files are in this directory.
<code>...../ScannerController.properties</code>	Configuration file for the ScannerController.
<code>...../ScannerControllerLogging.properties</code>	Properties file for the Scanner logging.
<code>...../scanner_typeScanner.cfg</code>	The configuration file for the connector. This file is copied to the <code>/scanner</code> directory before the child process is launched.
<code>.../logs</code>	Contains the log files for the ScannerController process.
<code>.../outgoing</code>	XML files that contain content and metadata are queued in this folder before they are sent to the Network Discover Server.

**Table 54-3** Installation directory structure (*continued*)

Path	Description
....../scanner	Binaries, the log files, and the temp files are under this directory.
...../outgoing	Some connectors (for example 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.

## 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	Configuration Tasks
<code>ScannerController.properties</code>	<p>In the <code>ScannerController.properties</code> file, you can configure the following options:</p> <ul style="list-style-type: none"> <li>■ Define Network Discover Server connection information.</li> <li>■ Provide content compression to reduce network load.</li> <li>■ Turn on and off incremental scanning. Additional configuration may be required in the <code>Vontusscanner_typeScanner.cfg</code> file.</li> </ul> <p>See <a href="#">“Scanner controller configuration options”</a> on page 958.</p>

File name	Configuration Tasks
<code>ScannerControllerLogging.properties</code>	<p>In the <code>ScannerControllerLogging.properties</code> file, you can configure the following options:</p> <ul style="list-style-type: none"> <li>■ Specify the logging levels from <code>.level = INFO</code> to <code>.level = FINEST</code>.</li> </ul>
<code>Vontusscanner_typeScanner.cfg</code>	<p>In the <code>Vontusscanner_typeScanner.cfg</code> file, you can configure the following options:</p> <ul style="list-style-type: none"> <li>■ Specify multiple jobs (run sequentially).</li> <li>■ Define access credentials. See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.</li> <li>■ Define filters.</li> <li>■ Define throttling.</li> <li>■ Specific settings are also available for each scanner type.</li> </ul>

## Scanner controller configuration options

Initial scanner configuration occurs during installation. Following installation, you can modify or specify additional scan settings.

[Table 54-4](#) provides an explanation of commonly modified parameters in the `ScannerController.properties` file.

**Table 54-4** Commonly modified parameters in `ScannerController.properties`

Parameter	Default	Description
<code>discover.host</code>	localhost	The hostname 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.
<code>discover.port</code>	8090	The Network Discover port to which the scanner routes data.

**Table 54-4** Commonly modified parameters in ScannerController.properties  
*(continued)*

Parameter	Default	Description
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.
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.

**Table 54-4** Commonly modified parameters in ScannerController.properties  
*(continued)*

Parameter	Default	Description
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 <i>scanner_typeScanner.cfg</i> 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 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 scanning of file systems

Scanning the file systems that are not file shares 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 951.

For file shares, use the server file system target.

See [“Setting up scans of file shares”](#) on page 899.

To set up scanning of file systems, complete the following process:

**Table 55-1**      Setting up a file system scanner

Step	Action	Description
Step 1	<p>Verify that your file system is on the list of supported targets.</p> <p>The file system scanner can scan local file systems on remote Windows, Linux, AIX, and Solaris servers.</p>	<p>See <a href="#">“Supported file system (scanner) targets”</a> on page 963.</p>
Step 2	<p>On the server that contains the file system, install the file system scanner.</p> <p>The setup for scanning file systems requires installation of the scanner software on the computer where the file system is located.</p> <p>On Linux, AIX, and Solaris, the root user must install the scanner.</p>	<p>See <a href="#">“Installing file system scanners”</a> on page 964.</p> <p>See <a href="#">“Installing file system scanners silently from the command line”</a> on page 967.</p>
Step 3	<p>Perform any manual configurations by editing the configuration files and properties files.</p>	<p>See <a href="#">“Configuration options for file system scanners”</a> on page 968.</p>
Step 4	<p>On the Enforce Server, add a new Scanner File System target.</p>	<p>See <a href="#">“Adding a new Network Discover target”</a> on page 850.</p>

**Table 55-1** Setting up a file system scanner (*continued*)

Step	Action	Description
Step 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 966.
Step 6	Verify that the scan is running successfully.	See “Troubleshooting scanners” on page 952.

## Supported file system (scanner) targets

The following remote Windows systems can be scanned:

- Windows 2000
- Windows 2003, 32-bit
- Windows XP, 32-bit

The following Linux file systems can be scanned:

- x86 32-bit, Red Hat Enterprise Linux AS 4

The following AIX file systems can be scanned:

- AIX 5.3

AIX requires the following C run time libraries, as well as Java 1.5:

- `x1C.aix50.rte (v8.0.0.0+)`
- `x1C.rte (v8.0.0.0+)`

The following Solaris file systems can be scanned:

- Solaris 8 (SPARC platform)
- Solaris 9 (SPARC platform)
- Solaris 10 (SPARC platform)

Solaris requires the following patch levels for the scanner:

- Solaris 8, 111308-05  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-111308-05-1>
- 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

- 1 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 `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` or `DLPDownloadHome/Symantec_DLP_11_Lin/Scanners` directory, where `DLPDownloadHome` 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:

- `FileSystemScanner_windows_x32_11.0.exe`

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

- `FileSystemScanner_Aix_11.0.sh`
- `FileSystemScanner_Unix_11.0.sh` (for Linux systems)

- `FileSystemScanner_Solaris_11.0.sh`

**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:

```
FileSystemScanner_windows_x32_11.0.exe
```

Linux GUI:

```
./FileSystemScanner_Unix_11.0.sh
```

Linux console:

```
./FileSystemScanner_Unix_11.0.sh -c
```

**3** Select the installation Destination Directory (the directory where you want the Vontu File System Scanner installed).

**4** For Windows, select the Start Menu Folder (shortcut in the **Start** menu). The default is **Vontu FileSystem Scanner**.

**5** Enter the following connection information for the Network Discover Server:

- Discover Host (IP or host name of the Network Discover Server)
- Discover Port

**6** 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.

**7** The scanner installs.

**8** 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.
- 9 The File Scanner installation is complete on the scanner computer.
  - 10 Perform any manual configurations by editing the configuration files and properties files.  
See “[Configuration options for file system scanners](#)” on page 968.  
See “[Scanner installation directory structure](#)” on page 955.  
See “[Scanner configuration files](#)” on page 957.
  - 11 On the Enforce Server, create a New Target for the scanner File System type.
  - 12 Start the scan on both the scanner computer and the Enforce Server.  
See “[Starting file system scans](#)” on page 966.

## 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 964.

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

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 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
```

- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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 file system scan with multiple scanners for one target**

- 1 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 955.
- 2 Log on to the Enforce Server.  
  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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.

## 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 964.

**To automate file scanner installation**

- 1 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
```

- 3 To run the installation with the `varfile`, type the following command (for Linux):

```
# ./FileSystemScanner_Unix_11.0.sh
-varfile FileSystemScanner.varfile -q
```

The parameter `-q` performs a silent installation.

## Configuration options for file system scanners

Table 55-2 provides a description of the primary parameters in the `VontuFileSystemScanner.cfg` file.

**Table 55-2** Parameters in the `VontuFileSystemScanner.cfg` file

Type	Parameter	Description
Scanned Content	DirectoryPathCSVs	Comma-separated list of directories to scan.

**Table 55-2** Parameters in the VontuFileSystemScanner.cfg file (*continued*)

Type	Parameter	Description
Scanned Content	DirectoryCantHaveCSVs	Exclude filters of the paths. Delimit entries with a comma, but do not use any spaces.
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 <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.

## Example configuration for scanning the C drive on a Windows computer

Scan the C drive on a Windows computer.

**Example configuration for scanning the /usr directory on UNIX**

This configuration is in the file `VontuFileSystemScanner.cfg`.

See [“Configuration options for file system scanners”](#) on page 968.

```
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 968.

```
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 968.

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 968.

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 968.

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 968.

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 968.

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 `VontuFileSystemScanner.cfg`.

See [“Configuration options for file system scanners”](#) on page 968.

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 Microsoft Exchange servers

This chapter includes the following topics:

- [Setting up scanning of Microsoft Exchange Servers](#)
- [Supported Exchange scanner targets](#)
- [Checking Exchange Mailbox Store permissions](#)
- [Installing Exchange scanners](#)
- [Configuration options for Exchange scanners](#)
- [Configuring the profile name](#)
- [Configuring settings for DNMailbox](#)
- [Starting Microsoft Exchange scans](#)
- [Example configuration for scanning the Exchange Archive Public Folder](#)
- [Example configuration for scanning an Exchange Inbox](#)
- [Example configuration for scanning another user's Inbox](#)
- [Example configuration for scanning all Exchange mailboxes](#)

## 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:

**Table 56-1**      Setting up an Exchange scanner

Step	Action	Description
Step 1	Verify that your Exchange server is on the list of supported targets.	See <a href="#">“Supported Exchange scanner targets”</a> on page 977.
Step 2	Install the Exchange scanner on any computer that has Microsoft Outlook 2003 or 2007 installed and a valid Outlook profile configured.	See <a href="#">“Installing Exchange scanners”</a> on page 979.
Step 3	Configure the <code>ProfileName</code> , and the setting for <code>DNMailbox</code> .	See <a href="#">“Configuring the profile name”</a> on page 984. See <a href="#">“Configuring settings for DNMailbox”</a> on page 985.
Step 4	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for Exchange scanners”</a> on page 981.
Step 5	On the Enforce Server, add a new Exchange target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.

**Table 56-1** Setting up an Exchange scanner (*continued*)

Step	Action	Description
Step 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 966.
Step 7	Verify that the scan is running successfully.	See “Troubleshooting scanners” on page 952.

## Supported Exchange scanner targets

The Exchange scanner supports scanning of the following targets:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007

Outlook 2003 or Outlook 2007 with a valid Outlook profile must be configured. The Exchange scanner uses Outlook to connect to the Exchange Server and fetch the data. Outlook 2003 or 2007 must be installed on the computer where the scanner is run. Outlook must be configured to talk to the Exchange server you want to scan.

Refer to the following link for steps to set up Outlook 2003 or Outlook 2007.

<http://support.microsoft.com/kb/829918>

The Exchange scan includes Exchange items in email file format (.EML files) and file attachments from the client’s mailbox, and scans the content of compressed files.

You can scan the data objects that are stored within the Public Folders.

The Exchange scanner does not, however, target the mail that is stored in Personal Folders (.pst files) or offline folders (.ost files). For scanning of .pst files, use the shared file system target.

See “Configuring scans of Microsoft Outlook Personal Folders (.pst files)” on page 901.

The Exchange scanner does not monitor the inbound messages or outbound messages that are sent with MAPI, SMTP, POP3, or HTML Web mail. POP3 or HTML Web mail scan types can be handled with other products of Symantec Data Loss Prevention.

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

See [“Implementing Network Monitor”](#) on page 803.

See [“Implementing Network Prevent \(Email\)”](#) on page 813.

## Checking Exchange Mailbox Store permissions

The Exchange scanner scans the mailboxes or public folders to which the Outlook profile has rights. For example, you can log on the client using Windows Administrator credentials and an Admin-level Outlook profile. Then you can scan all the mailboxes or public folders for which that profile has access. If you log on to Exchange using User A’s profile, you can only scan items for which User A has access, typically User A’s own mailbox.

When you scan other users’ mailboxes using an administrative account, that account must have access to all the mailboxes. The account must also have access to the Exchange server’s Mailbox Store object.

### To check the Mailbox Store permissions for Exchange 2003

- 1 Open the **Exchange System Manager**.
- 2 Find and right-click the **Mailbox Store** object.
- 3 Select **Properties**
- 4 Select the **Security** tab.

### To check the Mailbox Store permissions for Exchange 2007

- 1 Open the Exchange Management Shell.

[Exchange Management Shell](#) information at Microsoft.

Run the following command:

```
Add-ExchangeAdministrator -Role ViewOnlyAdmin -Identity MyDomain\My_User
```

- 2 Open the **Exchange Management Console**.  
[Exchange Management Console](#) information at Microsoft.
- 3 Under **Organization Configuration > Exchange Administrators > Actions**, select **Add Exchange Administrator**.
- 4 Select the user or group to add as an Exchange administrator. Select the role **Exchange View-Only Administrator role**.

# Installing Exchange scanners

Install the Exchange scanner on any Windows computer with Microsoft Outlook 2003 or Outlook 2007 installed and a valid Outlook profile.

The [Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL Security Update](#) must be installed on the computer running the Exchange scanner. If this runtime library is not installed, the Exchange scanner does not start.

When using `IndexAllAccounts=true`, you must use the profile of a user who has read permissions to all mailboxes. Check your permissions to the Exchange Mailbox Store.

See [“Checking Exchange Mailbox Store permissions”](#) on page 978.

## To install an Exchange scanner

- 1 Log on to the computer to install the Exchange scanner with a Windows Administrator account that has full access rights to all files.

The computer should be running Microsoft Outlook 2003 or Outlook 2007 with a valid Outlook profile, and have access to the Exchange server.

- 2 Download or copy (as binary) the installer (`ExchangeScanner_windows_x32_11.0.exe`) to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` where `DLPDownloadHome` is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

- 3 Run the Exchange scanner installer and follow the on-screen instructions.

- 4 On the Welcome screen, click **Next**.

- 5 Select the Destination Directory (the folder where you want the Vontu Exchange Scanner to be installed).

The default is `c:\Program Files\ExchangeScanner\`.

Click **Next**.

- 6 Select the Start Menu Folder (shortcut in the **Start** Menu).

The default is **Vontu Exchange Scanner**.

Click **Next**.

- 7 Enter the following connection information for the Network Discover Server:

- Discover Host (IP or hostname of the Network Discover Server)

- Discover Port.

Click **Next**.

- 8 Enter the following information to configure the connection to the Exchange Server.

- Profile Name

The MAPI profile (and associated privileges) you use to connect to the Exchange server for scanning

- Start Folder

The folder to scan (only applies when IndexAllAccounts=false, which is the default).

Click **Next**.

- 9 The scanner installs.

- 10 Select the Startup Mode.

The scanner must run as the same user as the one who owns the profile that is specified in the configuration file.

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.

To run as a service, after the installation is completed, you need to set the appropriate credentials for the service named **Vontu ExchangeScanner Service**.

On the computer where the scanner is installed, open the **Start > Settings > Control Panel > Administrative Tools > Services**. Find the local service named **Vontu ExchangeScanner Service**. Right-click this service, and select **Properties**. Click the **Log On** tab. Select **This account**. Then enter the user name and password of a user with the appropriate credentials.

- Start after installation.

- 11 Click **Next**, then click **Finish**.

12 Open and edit the file `VontuExchangeScanner.cfg`.

See [“Configuration options for Exchange scanners”](#) on page 981.

See [“Scanner installation directory structure”](#) on page 955.

The Exchange folder structure that is in the `Job0.log` file can be useful for figuring out what to use for the `StartFolder`. To see the Exchange folder structure, set the `ShowFolderStructure` parameter to true before you start the scanner.

13 Save your changes and close the configuration file.

14 Open the Enforce Server administration console in a Web browser and add a new Exchange target.

See [“Network Discover scan target configuration options”](#) on page 855.

15 Start the scan on both the scanner computer and the Enforce Server.

See [“Starting Microsoft Exchange scans”](#) on page 985.

## Configuration options for Exchange scanners

[Table 56-2](#) provides an explanation of the `VontuExchangeScanner.cfg` file.

**Table 56-2** Parameters in the `VontuExchangeScanner.cfg` file

Type	Parameter	Description
Scanned Content (public folders or single mailbox)	<code>ProfileName</code>	The name of the Microsoft Outlook profile which you want to connect to the Microsoft Exchange Server. The profile name may not be the same as the user name.  See <a href="#">“Configuring the profile name”</a> on page 984.

**Table 56-2** Parameters in the VontuExchangeScanner.cfg file (*continued*)

Type	Parameter	Description
Scanned Content (public folders or single mailbox)	StartFolder	<p>The folder from which to start fetching data. The StartFolder value is case-sensitive .</p> <p>No trailing slashes are allowed for the StartFolder value. Use IPM_SUBTREE\Inbox but not IPM_SUBTREE\Inbox\.</p> <p>The folder to scan only applies when IndexAllAccounts=false.</p> <p>The Exchange folder structure is in the Job0.log file. This folder structure can be useful for figuring out what to use for the value of the StartFolder parameter.</p> <p>The StartFolder value in the configuration depends on the Cached Exchange Mode that is configured for the profile.</p> <p>Cached Exchange Mode is a setting within Microsoft Outlook which affects the manner by which data is collected from a Microsoft Exchange Server. Running in cached mode prevents Outlook from constantly requesting new information from the server. See <a href="http://office.microsoft.com/en-us/outlook/CH010045991033.aspx">http://office.microsoft.com/en-us/outlook/CH010045991033.aspx</a></p> <p>In the Outlook profile, if the Cached Exchange Mode is false (not checked), then the "Top of Information Store" is the top folder for the mailbox. The StartFolder value for Inbox in this case is StartFolder=Top of Information Store\Inbox.</p> <p>If the Cached Exchange mode is set to true (checked), then IPM_SUBTREE is the root. The StartFolder value for Inbox in this case is StartFolder=IPM_SUBTREE\Inbox.</p>
Scanned Content (public folders or single mailbox)	Password	<p>The password for the MAPI profile.</p> <p>Passwords should be encrypted if they are stored in configuration files.</p> <p>See “<a href="#">Encrypting passwords in configuration files</a>” on page 861.</p>

**Table 56-2** Parameters in the VontuExchangeScanner.cfg file (*continued*)

Type	Parameter	Description
Scanned Content (public folders or single mailbox)	ShowFolderStructure	<p>If true, print the Exchange server folder structure to the Job0.log file (only applies when IndexAllAccounts=false).</p> <p>The default value of ShowFolderStructure is false.</p> <p>This folder structure can be useful for figuring out what to use for the value of the StartFolder parameter.</p> <p>If the Public Folder structure is large, a few hours may be necessary for the entire tree structure to be written to the log file. Another option is to use the Microsoft Exchange Server MAPI Editor to figure out the StartFolder value. See <a href="http://www.microsoft.com/downloads/details.aspx?FamilyID=55fdffd7-1878-4637-9808-1e21abb3ae37&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?FamilyID=55fdffd7-1878-4637-9808-1e21abb3ae37&amp;displaylang=en</a></p> <p>In most cases, ShowFolderStructure should be set to false after the folder structure has been determined.</p>
Scanned Content (public folders or single mailbox)	Incremental	<p>If true, only scan the messages that are new since the last scan. You must also set scanner.incremental=true in the ScannerController.properties file.</p> <p>The previous run of the scanner must have completed successfully for the incremental-mode scanner to run correctly. If the run was aborted before completion, the Incremental parameter cannot be used.</p>

**Table 56-2** Parameters in the VontuExchangeScanner.cfg file (*continued*)

Type	Parameter	Description
Scanned Content (all mailboxes)	IndexAllAccounts	If true, scan all mailboxes. The account that is specified with DNMailbox must have sufficient permissions. You must use the profile of a user who has read permissions to all mailboxes. This user does not need to be an Administrator.  Check your permissions to the Exchange Mailbox Store.  See <a href="#">“Checking Exchange Mailbox Store permissions”</a> on page 978.
Scanned Content (all mailboxes)	DNMailbox	The Distinguished Name of the mailbox or account that is used to log on to the server (only applies when IndexAllAccounts = true).  See <a href="#">“Configuring settings for DNMailbox”</a> on page 985.
Scanned Content (all mailboxes)	Mailbox	The Distinguished Name of the mailbox. Omit to scan all the mailboxes.
Throttling and Scan Control	BatchSize	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover.  See <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.

## Configuring the profile name

The Exchange scanner uses a configured Outlook profile to scan the Exchange server.

### To configure the profile name

- 1 Navigate to **Control Panel > Mail > Show Profiles**.
- 2 Locate the MAPI profile name for your Exchange configuration.
- 3 Enter the value for ProfileName in the VontuExchangeScanner.cfg file.

See [“Configuration options for Exchange scanners”](#) on page 981.

## Configuring settings for DNMailbox

Locate the values for `DNMailbox`, and configure the parameters in the `VontuExchangeScanner.cfg` file.

To configure the setting for `DNMailbox`

- 1 Download the Active Directory Services Interface (ADSI) Edit support tool from the following location.

<http://technet2.microsoft.com/windowsserver/en/library/ebca3324-5427-471a-bc19-9aa1decd3d401033.mspx?mfr=true>

- 2 Install the ADSI Edit support tool.

The ADSI Edit support tool is normally installed in the following location:

```
c:\Program Files\Support Tools\adsiedit.msc
```

- 3 To find the setting for the `DNMailbox` value, open the ADSI Edit application and locate the `DNMailbox` value.

For example, the value is the `legacyExchangeDN` attribute value of the Administrator User. The location may be different in your Exchange configuration.

Note that the `DNMailbox` value is case-sensitive

- 4 Enter the `DNMailbox` value in the `VontuExchangeScanner.cfg` file.

See “[Configuration options for Exchange scanners](#)” on page 981.

## Starting Microsoft Exchange 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 Exchange scanners](#)” on page 979.

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 an Exchange scan with one scanner for one target

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 On the scanner computer, start the Exchange scanner.  
Click **Start > Vontu Exchange Scanner > Vontu Exchange Scanner Console**.  
To run as a console, log into the computer using a valid user account, or use the `run as` command when launching the scanner.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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 an Exchange scan with multiple scanners for one target

- 1 On each of the scanner computers, start the Microsoft Exchange scanner.  
Click **Start > Vontu Exchange Scanner > Vontu Exchange Scanner Console**.  
To run as a console, log into the computer using a valid user account, or use the `run as` command when launching the scanner.  
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 955.
- 2 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.

- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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.

## Example configuration for scanning the Exchange Archive Public Folder

Scan the archive public folder.

This configuration is in the file `VontuExchangeScanner.cfg`.

See [“Configuration options for Exchange scanners”](#) on page 981.

```
//#####  
//# Jobs  
//#####  
[Jobs]  
Number=1  
0=Job0  
  
[Job0]  
ProfileName=Administrator  
Password=mypassword  
StartFolder=IPM_SUBTREE\Archive
```

## Example configuration for scanning an Exchange Inbox

Scan some-user profile’s Inbox.

This configuration is in the file `VontuExchangeScanner.cfg`.

See [“Configuration options for Exchange scanners”](#) on page 981.

```
//#####  
//# Jobs  
//#####  
[Jobs]  
Number=1  
0=Job0  
  
[Job0]
```

```
ProfileName=some-user  
Password=some-password  
StartFolder=IPM_SUBTREE\Inbox
```

## Example configuration for scanning another user's Inbox

With the Administrator profile, scan the Inbox of user TEST2.

Check your permissions to the Exchange Mailbox Store.

See [“Checking Exchange Mailbox Store permissions”](#) on page 978.

This configuration is in the file `VontuExchangeScanner.cfg`.

See [“Configuration options for Exchange scanners”](#) on page 981.

```
//#####  
//# Jobs  
//#####  
[Jobs]  
Number=1  
0=Job0  
  
[Job0]  
ProfileName=Administrator  
Password=myspassword  
  
IndexAllAccounts = true  
DNMailbox=/o=Dar Test Lab/ou=First Administrative Group  
/cn=Recipients/cn=Administrator  
  
Mailbox=/O=DAR TEST LAB  
/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS  
/CN=TEST2  
StartFolder=Top of Information Store\Inbox
```

## Example configuration for scanning all Exchange mailboxes

Scan all mailboxes.

Check your permissions to the Exchange Mailbox Store.

See [“Checking Exchange Mailbox Store permissions”](#) on page 978.

This configuration is in the file `VontuExchangeScanner.cfg`.

See [“Configuration options for Exchange scanners”](#) on page 981.

```
//#####  
//# Jobs  
//#####  
[Jobs]  
Number=1  
0=Job0  
  
[Job0]  
IndexAllAccounts=true  
ProfileName=Administrator  
Password=myspassword  
DNMailbox=/o=Dar Test Lab/ou=First Administrative Group  
/cn=Recipients/cn=Administrator
```



# Setting up scanning of SharePoint 2007 servers

This chapter includes the following topics:

- [Setting up scanning of SharePoint 2007 servers](#)
- [Supported SharePoint scanner targets](#)
- [Access privileges for a SharePoint 2007 scan](#)
- [Installing SharePoint 2007 scanners](#)
- [Starting SharePoint 2007 scans](#)
- [Configuration options for SharePoint 2007 scanners](#)
- [Example configuration for scanning a specific site collection](#)
- [Example configuration for scanning a specific Web site](#)
- [Example configuration for scanning all Web sites from a Web application](#)
- [Example configuration for scanning all Web sites from all Web applications present on the server](#)
- [Scheduling SharePoint 2007 scanning](#)

## Setting up scanning of SharePoint 2007 servers

The SharePoint 2007 scanner scans the head revision of documents and list items from Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007. The scanner then converts the files into a standard format and sends the files to the Network Discover Server for content processing.

The SharePoint 2007 scanner communicates with the SharePoint server through the Microsoft APIs. The scanner must be installed on one of the SharePoint 2007 Web Front End (WFE) servers because the Microsoft API limits the ability to communicate with the SharePoint server through its API. It can communicate only from the components that are installed directly on the SharePoint server.

See [“Supported SharePoint scanner targets”](#) on page 993.

See [“Access privileges for a SharePoint 2007 scan”](#) on page 994.

To set up scanning of SharePoint 2007 servers, complete the following process:

**Table 57-1**      Setting up a SharePoint 2007 scanner

Step	Action	Description
Step 1	Verify that your SharePoint 2007 server is on the list of supported targets.	See <a href="#">“Supported SharePoint scanner targets”</a> on page 993.
Step 2	Install the SharePoint 2007 scanner.  The setup for scanning SharePoint 2007 servers requires installation of the scanner software on one of the Web Front End (WFE) servers of a SharePoint 2007 deployment.	See <a href="#">“Installing SharePoint 2007 scanners”</a> on page 994.
Step 3	Set the access privileges to allow SharePoint scanning.	See <a href="#">“Access privileges for a SharePoint 2007 scan”</a> on page 994.
Step 4	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for SharePoint 2007 scanners”</a> on page 998.
Step 5	On the Enforce Server, add a new Scanner SharePoint 2007 target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.

**Table 57-1** Setting up a SharePoint 2007 scanner (*continued*)

Step	Action	Description
Step 6	<p>Start the SharePoint 2007 scan.</p> <p>Start the scanner on the SharePoint server, and also start the scan on the Enforce Server.</p>	See <a href="#">“Starting SharePoint 2007 scans”</a> on page 996.
Step 7	Verify that the scan is running successfully.	See <a href="#">“Troubleshooting scanners”</a> on page 952.

## Supported SharePoint scanner targets

The following SharePoint targets are supported for scanners:

- Microsoft Office SharePoint 2007 Server, on Windows Server 2003, 32-bit  
 Separate scanner installation is available for SharePoint 2007 32-bit servers. Use the following SharePoint scanner installation file for SharePoint 2007 32-bit servers:  
`SharePoint2007Scanner_windows_x32_11.0.exe`  
 See [“Setting up scanning of SharePoint 2007 servers”](#) on page 991.  
 The scanner must be installed on one of the Web Front End (WFE) servers of a SharePoint 2007 32-bit farm.  
 The Microsoft Visual C++ 2005 SP1 (32-bit) Redistributable Package must be installed on the computer.  
[Link to Microsoft 32-bit download.](#)
- Microsoft Office SharePoint 2007 Server, on Windows Server 2003, 64-bit, or Windows 2008 R1  
 Separate scanner installation is available for SharePoint 2007 64-bit servers. Use the following SharePoint scanner installation file for SharePoint 2007 64-bit servers.  
`SharePoint2007Scanner_windows_x64_11.0.exe`  
 See [“Setting up scanning of SharePoint 2007 servers”](#) on page 991.  
 The scanner must be installed on one of the Web Front End (WFE) computers of a SharePoint 2007 64-bit farm.  
 The Microsoft Visual C++ 2005 SP1 (64-bit) Redistributable Package must be installed on the computer.  
[Link to Microsoft 64-bit download.](#)
- SharePoint 2003

See “[Setting up scanning of SharePoint 2003 servers](#)” on page 1003.

Make sure the correct SharePoint scanner is installed for your version of SharePoint.

## Access privileges for a SharePoint 2007 scan

The scanner process must run under an account that has appropriate access to the SharePoint server.

The SharePoint 2007 Scanner account provides privileges for the Windows Service for the scanner. This account is used to provide access to SharePoint content with the Windows SharePoint Services API, and makes standard WSS API Object Model code calls to enumerate and retrieve SharePoint content in a read-only operation.

Microsoft requires these elevated rights for interaction with any Windows or console application as specified in the following Microsoft Technet article:

<http://support.microsoft.com/kb/935751/en-us>

For most Sharepoint environments, you can use the application pool account.

To scan an entire SharePoint 2007 server, make sure the user account under which the SharePoint 2007 scanner runs has the following rights:

- Local and farm administrator rights
- Database owner permissions to the content and to the configuration databases for SharePoint 2007
- Site collection administrator rights, or full control for all web applications
- Permissions to access all the resources on the SharePoint 2007 server

## Installing SharePoint 2007 scanners

The scanner must be installed on one of the Web Front End (WFE) servers of a SharePoint 2007 deployment.

Verify that the prerequisites are met.

See “[Supported SharePoint scanner targets](#)” on page 993.

**To install and deploy the SharePoint 2007 scanner**

- 1 Verify the version of the SharePoint repository and front end.  
 Make sure the correct SharePoint scanner is installed for your version of SharePoint.  
 See [“Supported SharePoint scanner targets”](#) on page 993.
- 2 Verify that the scanner process that runs the SharePoint 2007 scanner has appropriate access.  
 See [“Access privileges for a SharePoint 2007 scan”](#) on page 994.
- 3 On the computer that has the SharePoint 2007 WFE, download the scanner installation file.  
 For a 32-bit SharePoint 2007 server, download or copy (as binary) the file `SharePoint2007Scanner_windows_x32_11.0.exe` to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` where `DLPDownloadHome` is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.  
 For a 64-bit SharePoint 2007 server, use the file `SharePoint2007Scanner_windows_x64_11.0.exe`.
- 4 Start the scanner installation program on the SharePoint 2007 WFE.
- 5 Review the Welcome screen, and click **Next**.
- 6 Select the installation Destination Directory, the folder where you want the SharePoint 2007 Scanner to be installed.  
 The default is `c:\Program Files\SharePoint2007Scanner\`.  
 Click **Next**.
- 7 Select the Start Menu Folder (shortcut in the **Start** menu).  
 The default is **Vontu SharePoint2007 Scanner**.  
 Click **Next**.
- 8 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or hostname of the Network Discover Server)
  - Discover Port.
- 9 Click **Next**.
- 10 Configure the SharePoint 2007 Scanner by entering the following information:
  - Include Filters

The URL of a SharePoint object must include the string(s) specified here to be fetched for scanning. The filter only applies to the part of the URL up to, and including, the List URL. Delimit entries with a comma, but do not use any spaces.

■ **Exclude Filters**

If any of these strings appear in the URL of a SharePoint object, then that object is not fetched. Delimit entries with a comma, but do not use any spaces.

**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 SharePoint 2007 scanner installation is complete on the SharePoint 2007 WFE.

**14** Perform any manual configurations by editing the configuration files and properties files.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

See [“Scanner installation directory structure”](#) on page 955.

See [“Scanner configuration files”](#) on page 957.

**15** On the Enforce Server, create a New Target for the scanner SharePoint 2007 type.

See [“Adding a new Network Discover target”](#) on page 850.

**16** Start the scan on both the scanner computer and the Enforce Server.

See [“Starting SharePoint 2007 scans”](#) on page 996.

## Starting SharePoint 2007 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 SharePoint 2007 scanners”](#) on page 994.

Then, you can start the scan.

The procedures are different for each of the following scenarios:

- One scanner per target (first procedure).
- Multiple SharePoint scanners for one target (second procedure).

#### To start a SharePoint 2007 scan with one scanner for one target

- 1 Log on to the Enforce Server.

Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.

- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 On the scanner computer, start the SharePoint 2007 scanner.

Click **Start > Vontu SharePoint2007 Scanner > Vontu SharePoint2007 Scanner Console**.

The user that runs the SharePoint 2007 scanner must have the appropriate permissions.

See [“Supported SharePoint scanner targets”](#) on page 993.

- 4 The scanner starts the process of scanning data.

See [“How Network Discover scanners work”](#) on page 951.

- 5 If the scan does not progress normally, you can troubleshoot it.

See [“Troubleshooting scanners”](#) on page 952.

- 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 SharePoint 2007 scan with multiple SharePoint scanners for one target**

- 1 On each of the scanner computers, start the SharePoint 2007 scanner.

Click **Start > Vontu SharePoint2007 Scanner > Vontu SharePoint2007 Scanner Console**.

The user that runs the SharePoint 2007 scanner must have the appropriate permissions.

See [“Supported SharePoint scanner targets”](#) on page 993.

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 955.

- 2 Log on to the Enforce Server.

Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.

- 3 Select the target for the scanner, and click the Play icon for the selected target.

- 4 The scanner starts the process of scanning data.

See [“How Network Discover scanners work”](#) on page 951.

- 5 If the scan does not progress normally, you can troubleshoot it.

See [“Troubleshooting scanners”](#) on page 952.

- 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.

## Configuration options for SharePoint 2007 scanners

[Table 57-2](#) provides an explanation of the `VontuSharePoint2007Scanner.cfg` file.

**Table 57-2** Parameters in the `VontuSharePoint2007Scanner.cfg` file

Type	Parameter	Description
Scanned Content	<code>FetchMode</code>	Specifies the set of documents to be scanned.  0 - Fetch information from an individual site-collection (specified by <code>StartURL</code> ).  1 - Fetch information from all sites in a Web application (specified by <code>StartURL</code> ).  2 - Fetch all information from all Web applications.
Scanned Content	<code>StartURL</code>	Specifies the URL of the Web application or site collection where the scanner job starts.
Scanned Content	<code>SingleSiteName</code>	If specified, only sites with their <b>Title</b> matching this string are fetched.
Scanned Content	<code>MustHaveCSVs</code>	This parameter is the Include Filter. If none of these strings appear in the URL of a SharePoint object, then the object is not fetched. This filter only applies to the part of the URL up to and including the List URL.  Delimit entries with a comma, but do not use any spaces.
Scanned Content	<code>CantHaveCSVs</code>	This parameter is the Exclude Filter. If any of these strings appear in the URL of a SharePoint object, then that object is not fetched.  Delimit entries with a comma, but do not use any spaces.
Scanned Content	<code>MaximumJobTime</code>	The maximum number of seconds a scanner job is allowed to run before the job stops. When the job stops, its status is written to the status file.
Throttling	<code>ImportPoliteness</code>	Specify the amount of time (in milliseconds) that the import module should wait between importing documents.
Throttling	<code>BatchSize</code>	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover.  See <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.

## Example configuration for scanning a specific site collection

Scan a specific site collection.

The configuration is in the file `VontuSharePoint2007Scanner.cfg`.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

```
FetchMode=0
StartURL=http://sp2007/sites/Site1
SingleSiteName=Site_Title
```

## Example configuration for scanning a specific Web site

Scan a specific Web site.

The configuration is in the file `VontuSharePoint2007Scanner.cfg`.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

```
FetchMode=0
StartURL=http://sp2007/sites/Site1
SingleSiteName=Site_Title
```

## Example configuration for scanning all Web sites from a Web application

Scan all Web sites in the Web application `sp2007:3856`.

The configuration is in the file `VontuSharePoint2007Scanner.cfg`.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

```
FetchMode=1
StartURL=http://sp2007:3856
```

## Example configuration for scanning all Web sites from all Web applications present on the server

Scan all Web sites from all Web applications present on the server.

The configuration is in the file `VontuSharePoint2007Scanner.cfg`.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

```
FetchMode=2
```

## Scheduling SharePoint 2007 scanning

The following example shows how to schedule SharePoint 2007 scanning.

### To schedule SharePoint 2007 scanning

- 1 Add the parameter `MaximumJobTime` to the `Job0` section with the number of seconds that you want the job to run.
- 2 Set the `ImportPoliteness` if needed.
- 3 To run an example job, enter the following content into the file `VontuSharePoint2007Scanner.cfg`. This job runs for maximum of five hours with throttling set to 15 seconds between import of each document, with a batch size of 10.

See [“Configuration options for SharePoint 2007 scanners”](#) on page 998.

```
FetchMode=2
MaximumJobTime=18000
ImportPoliteness=15000
BatchSize=10
```

- 4 Edit the credentials for the **Vontu SharePoint2007Scanner Service** to use the Administrator credentials.
- 5 Create a batch file with the following contents:

```
net stop "Vontu SharePoint2007Scanner Service" &
net start "Vontu SharePoint2007Scanner Service"
```

- 6 Set the scanner to run in incremental mode by setting the parameter `scanner.incremental` value to `true` in the `ScannerController.properties` file.  
See [“Scanner controller configuration options”](#) on page 958.
- 7 Schedule a task using the Windows `Scheduled Task` to run the batch file every day at the desired time.
- 8 Schedule the Discover target on the Enforce Server to start at the same time.



# Setting up scanning of SharePoint 2003 servers

This chapter includes the following topics:

- [Setting up scanning of SharePoint 2003 servers](#)
- [Installing SharePoint 2003 scanners](#)
- [Starting SharePoint 2003 scans](#)
- [Configuration options for SharePoint 2003 scanners](#)
- [Example configuration for scanning all SharePoint 2003 sites](#)
- [Example configuration for scanning one SharePoint 2003 site](#)

## Setting up scanning of SharePoint 2003 servers

The SharePoint 2003 scanner scans the head revision of documents and list items in a SharePoint 2003 deployment.

See “[Supported SharePoint scanner targets](#)” on page 993.

To set up scanning of SharePoint 2003 servers, complete the following process:

**Table 58-1**      Setting up a SharePoint 2003 scanner

Step	Action	Description
Step 1	Verify that your SharePoint 2003 server is on the list of supported targets.	See “ <a href="#">Supported SharePoint scanner targets</a> ” on page 993.

**Table 58-1**      Setting up a SharePoint 2003 scanner (*continued*)

Step	Action	Description
Step 2	<p>Install the SharePoint 2003 scanner.</p> <p>The setup for scanning SharePoint 2003 servers requires installation of the scanner software on one of the front-end computers of a SharePoint 2003 deployment.</p>	See <a href="#">“Installing SharePoint 2003 scanners”</a> on page 1004.
Step 3	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for SharePoint 2003 scanners”</a> on page 1008.
Step 4	On the Enforce Server, add a new Scanner SharePoint 2003 target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 5	<p>Start the SharePoint 2003 scan.</p> <p>Start the scanner on the scanner computer, and also start the scan on the Enforce Server.</p>	See <a href="#">“Starting SharePoint 2003 scans”</a> on page 1006.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Troubleshooting scanners”</a> on page 952.

## Installing SharePoint 2003 scanners

The scanner must be installed on one of the front-end computers of a SharePoint 2003 deployment.

Verify that the prerequisites are met.

See [“Supported SharePoint scanner targets”](#) on page 993.

The scanner process must run under an account that has appropriate access to the SharePoint site(s).

### To install and deploy the SharePoint 2003 scanner

- 1 Verify the version of the SharePoint repository and front end.  
See [“Supported SharePoint scanner targets”](#) on page 993.
- 2 On the computer that has the SharePoint 2003 front end, download the installation file. Download or copy (as binary) the `SharePoint2003Scanner_windows_x32_11.0.exe` file to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` where `DLPDownloadHome` is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.
- 3 Start the scanner installation program on the SharePoint 2003 front end.  
`SharePoint2003Scanner_windows_x32_11.0.exe`

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

- 4 Review the Welcome screen, and click **Next**.
- 5 Select the installation Destination Directory, the folder where you want the SharePoint 2003 Scanner to be installed.  
The default is `c:\Program Files\SharePoint2003Scanner\`.  
Click **Next**.
- 6 Select the Start Menu Folder (shortcut in the **Start** menu).  
The default is **Vontu SharePoint2003 Scanner**.  
Click **Next**.
- 7 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or hostname of the Network Discover Server)
  - Discover Port.
- 8 Click **Next**.
- 9 Configure the SharePoint 2003 Scanner by entering the following information:
  - Include Filters  
The URL of a SharePoint object must include the string(s) specified here to be fetched for scanning. Delimit entries with a comma, but do not use any spaces.
  - Exclude Filters

If the string(s) specified here do not appear in the URL of a SharePoint object, it is not fetched for scanning. Delimit entries with a comma, but do not use any spaces.

**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.

The default is to start the scanner manually.

**12** The SharePoint 2003 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 SharePoint 2003 scanners”](#) on page 1008.

See [“Scanner installation directory structure”](#) on page 955.

See [“Scanner configuration files”](#) on page 957.

**14** Open the Enforce Server administration console in a Web browser, and create a New Target for the scanner SharePoint 2003 type.

**15** Start the scan on both the scanner computer and the Enforce Server.

See [“Starting SharePoint 2003 scans”](#) on page 1006.

## Starting SharePoint 2003 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 SharePoint 2003 scanners”](#) on page 1004.

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 SharePoint 2003 scan with one scanner for one target

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 On the scanner computer, start the SharePoint 2003 scanner.  
Click **Start > Vontu SharePoint2003 Scanner > Vontu SharePoint2003 Scanner Console**.

---

**Note:** The scanner process must run under an account that has appropriate access to the SharePoint site(s).

---

- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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 SharePoint 2003 scan with multiple scanners for one target

- 1 On each of the scanner computers, start the SharePoint 2003 scanner.  
Click **Start > Vontu SharePoint2003 Scanner > Vontu SharePoint2003 Scanner Console**.

---

**Note:** The scanner process must run under an account that has appropriate access to the SharePoint site(s).

---

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 955.

- 2 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.

- 4 The scanner starts the process of scanning data.  
See “[How Network Discover scanners work](#)” on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See “[Troubleshooting scanners](#)” on page 952.
- 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.

## Configuration options for SharePoint 2003 scanners

[Table 58-2](#) provides an explanation of the `VontuSharePoint2003Scanner.cfg` file.

**Table 58-2** Parameters in the `VontuSharePoint2003Scanner.cfg` file

Type	Parameter	Description
Scanned Content	<code>SharePointServer</code>	URL of the SharePoint server
Scanned Content	<code>FetchMode</code>	Specifies the set of documents to be scanned.  0 - Single site (specified by the <b>SingleSiteName</b> parameter)  1 - All sites
Scanned Content	<code>SingleSiteName</code>	Specifies the SharePoint site name of the documents to scan.
Scanned Content	<code>MustHaveCSVs</code>	The list that contains include filters for paths. Delimit entries with a comma, but do not use any spaces.
Scanned Content	<code>CantHaveCSVs</code>	The list that contains exclude filters for paths. Delimit entries with a comma, but do not use any spaces.
Scanned Content	<code>FileExtensionCSVs</code>	The list of file extensions. Delimit entries with a comma, but do not use any spaces.
Authentication	<code>Username</code>	The Windows user name of a user who can download the documents from SharePoint.

**Table 58-2** Parameters in the `VontuSharePoint2003Scanner.cfg` file  
*(continued)*

Type	Parameter	Description
Authentication	Password	The password for the user that is specified in the Username parameter. Encrypt this password.  See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
Authentication	Domain	The domain of the user that is specified in the Username parameter.
Throttling	BatchSize	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover.  See <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.

## Example configuration for scanning all SharePoint 2003 sites

Scan all sites with filtering.

The configuration is in the file `VontuSharePoint2003Scanner.cfg`.

See [“Configuration options for SharePoint 2003 scanners”](#) on page 1008.

```
//#####
//# Jobs
//#####
[Jobs]
Number=1
0=Job0
[Job0]
SharePointServer = http://sharepoint_name.domain
MustHaveCSVs     = Document Library
CantHaveCSVs     = _catalogs
FetchMode = 1
```

## Example configuration for scanning one SharePoint 2003 site

Scan a single site.

The configuration is in the file `VontuSharePoint2003Scanner.cfg`.

See [“Configuration options for SharePoint 2003 scanners”](#) on page 1008.

```
//#####  
//# Jobs  
//#####  
[Jobs]  
Number=1  
0=Job0  
[Job0]  
SharePointServer = http://sharepoint_name.domain  
FetchMode = 0  
SingleSiteName = TestSite
```

# Setting up scanning of Web servers

This chapter includes the following topics:

- [Setting up 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 scanning of Web servers

The Web server scanner can retrieve Web site documents.

The Web server scanner uses spiders to find Web pages and to process the Web pages for content and links to other Web sites. Once a spider has finished retrieving documents from the Web site, the Web server scanner imports the content that the spider 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 spiders Web pages for links and content. The spider processes the page content and either accepts or rejects the page for retrieval. If the page is accepted, the spider looks for links from the page, filters the links and queues the accepted links for the spider process. If the page is rejected, the spider 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 spider queue. The spider then retrieves the page content of accepted pages. The spider requests the next link in its queue, and the process repeats.

To set up scanning of Web servers, complete the following process:

**Table 59-1**      Setting up a Web server scanner

Step	Action	Description
Step 1	The Web server scanner can scan Web sites.  It has been tested with IIS and Apache Web servers.	See <a href="#">“Supported Web server (scanner) targets”</a> on page 1013.
Step 2	On the server with read access to the Web site, install the Web server scanner.	See <a href="#">“Installing Web server scanners”</a> on page 1013.
Step 3	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for Web server scanners”</a> on page 1016.
Step 4	On the Enforce Server, add a new Scanner File System target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 5	Start the file system scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See <a href="#">“Starting Web server scans”</a> on page 1015.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Troubleshooting scanners”</a> on page 952.

# 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

- 1 On the computer that has access to the Web sites that you want to scan, download or copy (as binary) the installation file to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` or `DLPDownloadHome/Symantec_DLP_11_Lin/Scanners` directory, where `DLPDownloadHome` is the name of the directory in which you unzipped the Symantec Data Loss Prevention software.

If you install the Web server scanner on a Windows computer, use the following file:

```
WebServerScanner_windows_x32_11.0.exe
```

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

If you install the Web server scanner on a Linux computer, use the following file:

```
WebServerScanner_Unix_11.0.sh
```

- 2 Start the scanner installation.
- 3 Select the installation **Destination Directory** (the directory where you want the Web server scanner installed).

Click **Next**.

- 4 Select the Start Menu Folder (shortcut in the **Start** menu). The default is **Vontu WebServer Scanner**.

Click **Next**.

- 5 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**.

6 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 string(s) 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 string(s) specified here are scanned. Delimit entries with a comma, but do not use any spaces. Wildcards are supported.

Click **Next**.

7 The scanner installs.

8 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**.

9 The Web server scanner installation is complete on the scanner computer.

10 Perform any manual configurations by editing the configuration files and properties files.

See [“Configuration options for Web server scanners”](#) on page 1016.

See [“Scanner installation directory structure”](#) on page 955.

See [“Scanner configuration files”](#) on page 957.

11 On the Enforce Server, create a **New Target** for the scanner Web server type.

12 Start the scan on both the scanner computer and the Enforce Server.

See [“Starting Web server scans”](#) on page 1015.

# 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 1013.

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

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the play icon for the selected target.
- 3 On the scanner computer, start the Web server scanner.  
Click **Start > Vontu WebServer Scanner > Vontu WebServer Scanner Console**.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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

- 1 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 955.
- 2 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.

- 4 The scanner starts the process of scanning data.  
See “[How Network Discover scanners work](#)” on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See “[Troubleshooting scanners](#)” on page 952.
- 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.

## Configuration options for Web server scanners

Table 59-2 provides an explanation of the `VontuWebServerScanner.cfg` file.

Table 59-2 Parameters in the `VontuWebServerScanner.cfg` file

Type	Parameter	Description
Scanned Content	URL	A valid URL at which the spider 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 <code>http://</code> 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 <code>NavDirCheck</code> 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 <code>NavDirCheck</code> 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.

**Table 59-2** Parameters in the VontuWebServerScanner.cfg file (*continued*)

Type	Parameter	Description
Scanned Content	NavDirCheck	<p>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 NavDirDisallowCSVs strings, the scanner does not process the page.</p> <p>See <a href="#">“Example of URL filtering for a Web site scan”</a> on page 1021.</p>
Scanned Content	Extensions	<p>Enter file extensions to restrict the document types the scanner can spider. To enter multiple extensions, separate them with commas . Use * for wildcard. No spaces before or after commas.</p> <p>Example to only fetch the documents that have .doc or .html as extensions:</p> <pre>Extensions=*.doc,* .html*</pre>
Scanned Content	MaxLinksPerPage	<p>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.</p>
Scanned Content	StayOnSite	<p>You can configure the spider 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 spider stays on the starting Web site domain.</p>
Scanned Content	AfterDate	<p>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.</p>

**Table 59-2** Parameters in the VontuWebServerScanner.cfg file (*continued*)

Type	Parameter	Description
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.
Authentication	LoginMethod	The authentication method for the site. The value must be AUTHENTICATE, FORMPOST, or FORMGET.  See <a href="#">“Example configuration for a Web site scan with basic authentication”</a> on page 1019.  See <a href="#">“Example configuration for a Web site scan with form-based authentication”</a> on page 1020.
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 <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
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 <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
Proxies	ProxyHost	The hostname 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.

**Table 59-2** Parameters in the VontuWebServerScanner.cfg file (*continued*)

Type	Parameter	Description
Proxies	ProxyPassword	The password for the proxy server. Encrypt this password.  See “ <a href="#">Encrypting passwords in configuration files</a> ” on page 861.
Throttling	PageDelay	Number of seconds between downloading a page and requesting the next page.
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 1016.

```
//#####
//#   Jobs
//#####
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 1016.

```
//#####
//#   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 1016.

```
//#####  
//#   Jobs  
//#####  
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 `VontuWebServerScanner.cfg`.

See [“Configuration options for Web server scanners”](#) on page 1016.

```
//#####  
//#   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 <code>NavDirAllowCSVs</code> or <code>NavDirDisallowCSVs</code> .
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 <code>NavDirAllowCSVs</code> or <code>NavDirDisallowCSVs</code> . 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 <code>NavDirAllowCSVs</code> or <code>NavDirDisallowCSVs</code> 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 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 scanning of Documentum repositories

The Documentum scanner scans Documentum repositories.

To set up scanning of Documentum repositories, complete the following process:

**Table 60-1**      Setting up a Documentum scanner

Step	Action	Description
Step 1	Verify that your Documentum repository is on the list of supported targets.	See “ <a href="#">Supported Documentum (scanner) targets</a> ” on page 1024.

**Table 60-1**      Setting up a Documentum scanner (*continued*)

Step	Action	Description
Step 2	The Documentum scanner can be installed on any computer that has network connectivity to the computer that hosts the Documentum Document Broker.	See <a href="#">“Installing Documentum scanners”</a> on page 1024.
Step 3	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for Documentum scanners”</a> on page 1028.
Step 4	On the Enforce Server, add a new Scanner Documentum target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 5	Start the Documentum scan. Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See <a href="#">“Starting Documentum scans”</a> on page 1027.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Troubleshooting scanners”</a> on page 952.

## Supported Documentum (scanner) targets

The Documentum scanner supports scanning a Documentum Content Server 5.3.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

- 1 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 `DocumentumScanner_windows_x32_11.0.exe` file to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` where `DLPDownloadHome` 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.

`DocumentumScanner_windows_x32_11.0.exe`

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

- 3 Review the Welcome screen, and click **Next**.
- 4 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**.
- 5 Select the Start Menu Folder (shortcut in the **Start** menu).  
The default is **Vontu Documentum Scanner**.  
Click **Next**.
- 6 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or hostname of the Network Discover Server)
  - Discover Port
- 7 Click **Next**.

**8** Enter the following Documentum configuration values for the scanner:

<b>Doc Broker Host</b>	The name of the server where the repository for the DocBase is stored.
<b>Doc Base</b>	The name of the repository you want the Documentum scanner to retrieve.
<b>User Name</b>	Specify an account with full access rights to the Documentum files you want to scan.
<b>Password</b>	Password for the account. This password is plain text in the configuration file.
<b>WebTop Host</b>	The host name of the Web interface to the Documentum content repository.
<b>WebTop Port</b>	The port number for the Web interface.

**9** 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.

The default is to start the scanner manually.

**12** The Documentum 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 Documentum scanners”](#) on page 1028.

See [“Scanner installation directory structure”](#) on page 955.

See [“Scanner configuration files”](#) on page 957.

**14** 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 955.

- 15 On the Enforce Server, create a New Target for the scanner Documentum type.
- 16 Start the scan on both the scanner computer and the Enforce Server.  
See [“Starting Documentum scans”](#) on page 1027.

## 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 1024.

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

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 On the scanner computer, start the Documentum scanner.  
Click **Start > Vontu Documentum Scanner > Vontu Documentum Scanner Console**.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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**

- 1 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 955.
- 2 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.
- 4 The scanner starts the process of scanning data.  
See “[How Network Discover scanners work](#)” on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See “[Troubleshooting scanners](#)” on page 952.
- 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.

## Configuration options for Documentum scanners

[Table 60-2](#) provides an explanation of the `VontuDocumentumScanner.cfg` file.

**Table 60-2** Parameters in the `VontuDocumentumScanner.cfg` file

Parameter	Description
<code>DocBase</code>	The name of the repository you want Documentum to retrieve.
<code>UserName</code>	Specify an account with access rights to the Documentum files you want to scan.
<code>Password</code>	Password for the account that is specified in <b>UserName</b> . Encrypt this password. See “ <a href="#">Encrypting passwords in configuration files</a> ” on page 861.

**Table 60-2** Parameters in the `VontuDocumentumScanner.cfg` file (*continued*)

Parameter	Description
ExtensionCSVs	<p>List of file types to scan (Include Filter), for example:</p> <pre>ExtensionCSVs=*.doc,*.htm,*.ppt,*.xls</pre> <p>Delimit with a comma (no space).</p>
ImportRefReplaceWithCSVs	<p>Comma-separated list of one or two values that are used to construct the URL of the scanned documents.</p> <p><i>first_value,second_value</i></p> <p>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:</p> <p><i>first_valuedocument_idsecond_value</i></p> <p>If the Documentum Webtop (Web-based) interface is your client interface, only one value is necessary; for example:</p> <pre>ImportRefReplaceWithCSVs= http://documentum-server.mycompany.com:8080/ webtop/component/drl?objectId=</pre>
AfterDate	<p>A maximum age for documents to be scanned. For example, if you set <code>AfterDate</code> to 5 days, only documents that are no more than five days old are scanned. <code>AfterDate</code> looks at the last modified date.</p> <p>You can enter one of the following values:</p> <ul style="list-style-type: none"> <li><i>N</i> hours</li> <li><i>N</i> days</li> <li><i>N</i> weeks</li> <li><i>N</i> months</li> </ul> <p>The Documentum scanner does not support automatic incremental scanning, but you can manually perform incremental scans, by setting the <code>AfterDate</code> and <code>BeforeDate</code> parameters.</p>

**Table 60-2** Parameters in the `VontuDocumentumScanner.cfg` file (*continued*)

Parameter	Description
<code>BeforeDate</code>	<p>A minimum age for documents to be scanned. For example, if you set <code>AfterDate</code> to 5 days, only documents that are no more than five days old are scanned. <code>AfterDate</code> looks at the last modified date.</p> <p>You can enter one of the following values:</p> <ul style="list-style-type: none"> <li><code>N hours</code></li> <li><code>N days</code></li> <li><code>N weeks</code></li> <li><code>N months</code></li> </ul>
<code>FolderCSVs</code>	<p>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:</p> <p><code>FolderCSVs=/support,/clients,/marketing,/finance</code></p>

**Table 60-3** 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 60-3** `dmcl.ini` file

Parameter	Description
<code>host</code>	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`.

**Example configuration for scanning all documents in a Documentum repository**

See “[Configuration options for Documentum scanners](#)” on page 1028.

```
//#####  
//#   Jobs  
//#####  
[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
```

**Example configuration for scanning all documents in a Documentum repository**

# Setting up scanning of Livelink repositories

This chapter includes the following topics:

- [Setting up 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 scanning of Livelink repositories

The Livelink scanner can scan a Livelink database.

To set up scanning of Livelink repositories, complete the following process:

**Table 61-1**      Setting up a Livelink scanner

Step	Action	Description
Step 1	Verify that your Livelink repository is on the list of supported targets.	See <a href="#">“Supported Livelink (scanner) targets”</a> on page 1034.

**Table 61-1**      Setting up a Livelink scanner (*continued*)

Step	Action	Description
Step 2	Create an ODBC data source for SQL Server.  Install the Livelink scanner.	See <a href="#">“Creating an ODBC data source for SQL Server”</a> on page 1034.  See <a href="#">“Installing Livelink scanners”</a> on page 1035.
Step 3	Perform any manual configurations by editing the configuration files and properties files.	See <a href="#">“Configuration options for Livelink scanners”</a> on page 1039.
Step 4	On the Enforce Server, add a new Scanner Livelink target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 5	Start the Livelink scan.  Start the scanner on the scanner computer, and also start the scan on the Enforce Server.	See <a href="#">“Starting Livelink scans”</a> on page 1037.
Step 6	Verify that the scan is running successfully.	See <a href="#">“Troubleshooting scanners”</a> on page 952.

## Supported Livelink (scanner) targets

The Livelink scanner supports scanning of the following targets:

- Livelink Server 9.x

## Creating an ODBC data source for SQL Server

This procedure assumes that the Livelink database is a 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)**.
- 2**    Click the **System DSN** tab.
- 3**    Click **Add**.

- 4 Select **SQL Server**.
- 5 Give it a name (for example, “Livelink”). This name is referenced in the `VontuLiveLinkScanner.cfg` file.
- 6 Click **Next**.
- 7 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 1034.
- 2 On the computer that has access to the Livelink database, download the installation file. Download or copy (as binary) the `LivelinkScanner_windows_x32_11.0.exe` file to a temporary directory. The file is located in the `DLPDownloadHome\Symantec_DLP_11_Win\Scanners` where `DLPDownloadHome` 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.

`LivelinkScanner_windows_x32_11.0.exe`

---

**Note:** This scanner should only be installed on 32-bit Windows servers.

---

- 4 Review the Welcome screen, and click **Next**.
- 5 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**.

- 6 Select the Start Menu Folder (shortcut in the **Start** menu).  
The default is **Vontu Livelink Scanner**.  
Click **Next**.
- 7 Enter the following connection information for the Network Discover Server:
  - Discover Host (IP or hostname of the Network Discover Server)
  - Discover Port

Click **Next**.

- 8 Enter the following Livelink configuration values for the scanner:

<b>LiveLink Host</b>	The host name or IP address of the Livelink server.
<b>LiveLink Port</b>	The HTTP port of the Livelink server.
<b>LiveLink User Name</b>	The user name to use when you scan.
<b>LiveLink Password</b>	The password to use when you scan. Encrypt this password. See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
<b>LiveLink Connection Name</b>	The Livelink API connection name. This name is the <code>dbconnection</code> in the <code>opentext.ini</code> file on the Livelink server.
<b>LiveLink API Port</b>	This port should be 2099 unless it has been changed in the <code>opentext.ini</code> file on the Livelink server. The default is 2099.
<b>ODBC DSN</b>	The name of the ODBC data source on the computer running the Livelink scanner.
<b>SQL User Name</b>	User name to use to connect to the ODBC data source.
<b>SQL Password</b>	Password to use to connect to the ODBC data source. Encrypt this password. See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.

Click **Next**.

- 9 The scanner installs.
- 10 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.

- 11 The Livelink scanner installation is complete on the scanner computer.
- 12 Perform any manual configurations by editing the configuration files and properties files.  
See [“Configuration options for Livelink scanners”](#) on page 1039.  
See [“Scanner installation directory structure”](#) on page 955.  
See [“Scanner configuration files”](#) on page 957.
- 13 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`
- 14 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 1034.
- 15 On the Enforce Server, create a New Target for the scanner Livelink type.
- 16 Start the scan on both the scanner computer and the Enforce Server.  
See [“Starting Livelink scans”](#) on page 1037.

## 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 1035.

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**

- 1 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 2 Select the target for the scanner, and click the Play icon for the selected target.
- 3 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 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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 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 955.
- 2 Log on to the Enforce Server.  
Select **Manage > Discover Scanning > Discover Targets** to navigate to the list of targets.
- 3 Select the target for the scanner, and click the Play icon for the selected target.
- 4 The scanner starts the process of scanning data.  
See [“How Network Discover scanners work”](#) on page 951.
- 5 If the scan does not progress normally, you can troubleshoot it.  
See [“Troubleshooting scanners”](#) on page 952.
- 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.

# Configuration options for Livelink scanners

Table 61-2 provides an explanation of the `VontuLiveLinkScanner.cfg` file.

**Table 61-2** Parameters in the `VontuLiveLinkScanner.cfg` file

Type	Parameter	Description
Connectivity	<code>OpenTextServer</code>	The host name or IP address of the Livelink server.
Connectivity	<code>OpenTextPort</code>	The HTTP port of the Livelink server.
Connectivity	<code>OpenTextUsername</code>	The user name to use when you scan.
Connectivity	<code>OpenTextPassword</code>	The password to use when you scan. Encrypt this password. See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
Connectivity	<code>LLConnection</code>	The Livelink API connection name. This parameter is the name of the <code>dbconnection</code> in the <code>opentext.ini</code> file on the Livelink server.
Connectivity	<code>LLApiPort</code>	This value should be 2099 unless it has been changed in the <code>opentext.ini</code> file on the Livelink server.
Connectivity	<code>DSN</code>	The name of the ODBC data source on the computer that runs the Livelink scanner.
Connectivity	<code>SQLUserName</code>	User name to use to connect to the ODBC data source.
Connectivity	<code>SQLPassword</code>	Password to use to connect to the ODBC data source. Encrypt this password. See <a href="#">“Encrypting passwords in configuration files”</a> on page 861.
Throttling	<code>BatchSize</code>	The number of files that are aggregated before they are imported into each XML file that is sent to Network Discover. See <a href="#">“Optimizing resources with Network Discover scan throttling”</a> on page 868.

## 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 1039.

```
//#####  
//#   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=lldbuser  
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 the 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 1042.

An example of a Java SOAP client is available.

See [“Example of a Web Services Java client”](#) on page 1042.

To set up custom Web Services for Network Discover, complete the following process:

**Table 62-1**      Setting up a custom scan target

Step	Action	Description
Step 1	Add a Web Services target type.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.

**Table 62-1**      Setting up a custom scan target (*continued*)

Step	Action	Description
Step 2	Start the scan.	Click the play icon to start the scan.  See “ <a href="#">Managing Network Discover target scans</a> ” on page 874.
Step 3	Save and modify the WSDL, and create a client (such as a Java client), or SOAP request.	See “ <a href="#">About setting up the Web Services Definition Language (WSDL)</a> ” on page 1042.  An example Java client is available.  See “ <a href="#">Example of a Web Services Java client</a> ” on page 1042.
Step 4	Run the client, and verify the results.	See “ <a href="#">Example of a Web Services Java client</a> ” on page 1042.

## 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

- 1 Log into the Enforce Server and create a Network Discover Web Services target type.  
  
See “[Adding a new Network Discover target](#)” on page 850.  
  
Use the default settings. Note the scanner port number; the default is 8090.
- 2 Start the scan.

- 3 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.

- 4 Install the Java Development Kit (JDK), if it is not available on your system.
- 5 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 1043.

- 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 1042.

```
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 within 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 =
        new ComponentContentType();
    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)
{
}
}
}
```

# Discovering and preventing data loss on endpoint computers

- [Chapter 63. Using Endpoint Discover and Endpoint Prevent](#)
- [Chapter 64. Implementing Endpoint Discover](#)
- [Chapter 65. Implementing Endpoint Prevent](#)
- [Chapter 66. Working with agent configurations](#)
- [Chapter 67. Working with Endpoint FlexResponse](#)
- [Chapter 68. Implementing Symantec DLP Agents](#)
- [Chapter 69. Managing Symantec DLP Agents](#)
- [Chapter 70. About application monitoring](#)
- [Chapter 71. Using Endpoint Server tools](#)



# Using Endpoint Discover and Endpoint Prevent

This chapter includes the following topics:

- [About Endpoint Discover and Endpoint Prevent](#)
- [About Endpoint Prevent monitoring](#)
- [About Endpoint Discover monitoring](#)
- [About policies for endpoint computers](#)
- [About policy creation for Endpoint Prevent](#)
- [About rules results caching \(RRC\)](#)
- [About Endpoint reports](#)

## About Endpoint Discover and Endpoint Prevent

Endpoint Discover and Endpoint Prevent are related products that operate directly on an endpoint computer. Endpoint Discover and Endpoint Prevent 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, identification numbers. The type of data that can be considered sensitive is unlimited. You must define the type of sensitive information through a series of policies.

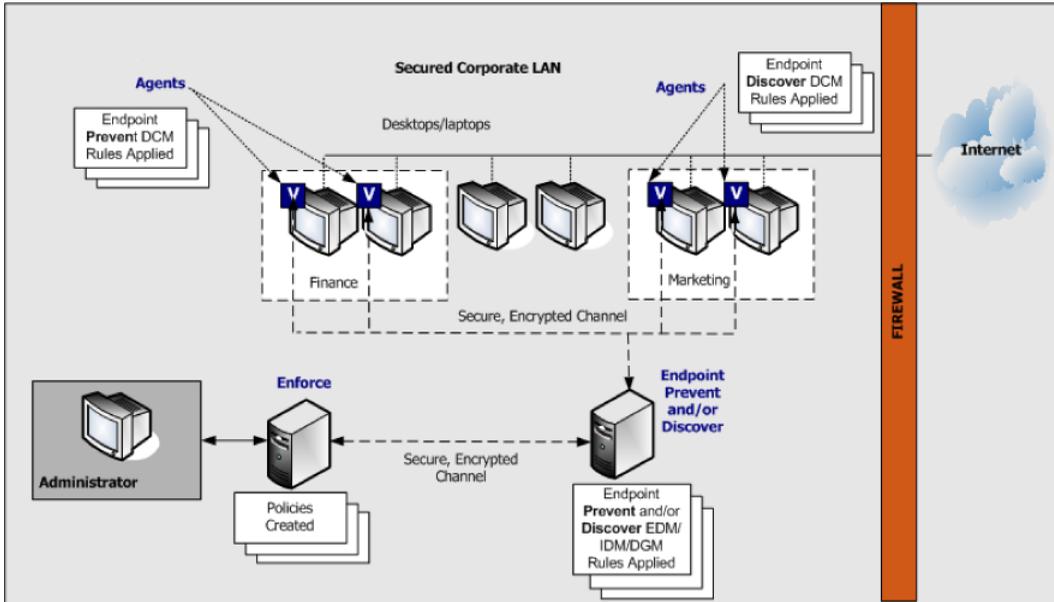
See [“Implementing policies”](#) on page 317.

Endpoint Discover scans endpoint computers to find the information that you have defined as at risk or sensitive. Endpoint Prevent stops sensitive data from moving off an endpoint computer. For example, Endpoint Prevent stops a file that contains credit card numbers from being transferred to a USB or FireWire

connected media. Endpoint Discover, however, examines the c: drive and locates every file that contains those credit card numbers that match a policy. Both of these products are configured to recognize the files that contain sensitive data and both products protect that data.

Endpoint Discover and Prevent are deployed using s and Endpoint Servers.

Figure 63-1 Secured Corporate LAN



## How Endpoint Discover works

Endpoint Discover lets you examine a hard drive in your organization for any data that is a potential risk. Endpoint Discover can only examine the main hard drive, such as the c: drive. 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 fixed drive that is connected to the endpoint computer such as the endpoint hard drive or external hard drives. It cannot scan CD/DVD drives or removable media devices such as a flash drive or SD card.

See “[About Endpoint Discover monitoring](#)” on page 1059.

## How Endpoint Prevent works

Endpoint Prevent interacts with policy groups and policies. Before you create policies, you must first create policy groups. The Endpoint Prevent policies are associated with these policy groups. 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 detects the activity that violates a policy rule, it generates an incident. The incident appears in your endpoint incident lists. You can respond to the incident by sending out an alert, notifying the endpoint user, and so on.

---

**Note:** Policy groups that are assigned to an Endpoint Server apply equally to all connected agents.

---

Symantec Data Loss Prevention can detect violations at the endpoint in a variety of ways including:

- Network events (HTTP/HTTPS, instant messaging , Email, FTP)
- CD/DVD events
- Network share events
- USB events (flash cards, SD cards)
- Print/Fax events
- Clipboard events

See [“About Endpoint Prevent monitoring”](#) on page 1052.

See [“About the Symantec DLP Agent”](#) on page 1052.

See [“Implementing policies”](#) on page 317.

## About the Endpoint Server

The Endpoint Server connects all of the Symantec DLP Agents that are deployed on your endpoint computers to the Enforce Server. The Endpoint Server also contains the detection policies for Endpoint Discover.

The Endpoint Server connects both Endpoint Discover and Endpoint Prevent.

Depending on your license, not every topic that is discussed in this guide may be applicable to your needs. For example, if you have licensed Endpoint Prevent, then you must configure the Endpoint Server to allow for monitoring and prevent

capabilities. However, if you have only licensed Endpoint Discover, you do not need to configure network capabilities.

See [“About Endpoint Discover and Endpoint Prevent”](#) on page 1049.

## About the Symantec DLP Agent

You deploy the Symantec DLP Agent on each endpoint computer you want to scan. An Enforce Server controls the Symantec DLP Agent and applies the policies and rules of that Endpoint Server. You cannot make individual changes to the Symantec DLP Agents.

The Symantec DLP Agent contains an encrypted data store, called the Agent Store. It acts as a buffer or holding space for the incidents and files that the Symantec DLP Agent sends to the Endpoint Server. If the Symantec DLP Agent is disconnected from the Endpoint Server, the Agent Store holds the incidents and files until connection is re-established. The Agent Store is limited in size (the default is 5% of disk space). If the maximum size is reached, the Symantec DLP Agent evicts files and incidents from the Agent Store. Eviction policies target the oldest files first, and then the oldest incidents. Files are targeted first because the file may or may not contain the sensitive data that the Endpoint Server must analyze. However, an incident is a direct violation of policies and a record of that violation must be retained if at all possible.

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about the endpoint computer operating systems on which you can install the Symantec DLP Agent.

See [“About preinstallation steps for Symantec DLP Agents”](#) on page 1104.

## About Endpoint Prevent monitoring

You can perform many different types of monitoring with Endpoint Prevent. Taken together, the different types of monitoring create the Endpoint Prevent product. The following table provides references to the types of monitoring you can perform.

**Table 63-1** Endpoint Prevent Monitoring

Type of Monitoring
<a href="#">About removable media monitoring</a>
<a href="#">About Endpoint network monitoring</a>
<a href="#">About CD/DVD monitoring</a>

**Table 63-1** Endpoint Prevent Monitoring (*continued*)

Type of Monitoring
<a href="#">About print/fax monitoring</a>
<a href="#">About network share monitoring</a>
<a href="#">About clipboard monitoring</a>
<a href="#">About application monitoring</a>

Endpoint Prevent monitors the activity on an endpoint computer regardless if it is connected to an Endpoint Server. If an endpoint computer is off of the network and cannot connect to an Endpoint Server, Endpoint Prevent continues to monitor the endpoint computer. All incidents are stored in the Agent Store until the computer is re-connected to the Endpoint Server. If the Agent Store exceeds the specified size limit, older files are ejected until the size limits are reached. Endpoint Prevent does not stop monitoring the endpoint computer.

See [“About the Symantec DLP Agent”](#) on page 1052.

## About removable media monitoring

Endpoint Prevent lets you block data transferring from your hard drive to a removable media device. Removable media includes the following devices:

- USB flash drive
- SD card
- Compact flash card
- FireWire connected device

When the Symantec DLP Agent detects that a violation has occurred, the data is not transferred. An incident is created and sent to the Endpoint Server. When a violation occurs, the Symantec DLP Agent displays a pop-up notification to the user that informs the user that the violation 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 747.

For example, User 1 copies a Microsoft Word file that contains medical records from an endpoint computer 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 violation 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 1052.

## 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 guarantee 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 endpoint computers”](#) on page 1060.

See [“About Endpoint Prevent monitoring”](#) on page 1052.

## About print/fax monitoring

Endpoint Prevent lets you monitor and prevent sensitive information from being either printed or faxed to a recipient. Within Windows, the mechanism for printing and faxing information is identical, therefore, the Endpoint Prevent mechanism is also identical.

Files are sent to the printer or the fax machine in pages and each page is then printed or faxed. Endpoint Prevent analyzes each page as it is sent to the printer or the fax machine. This means that some 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. The file is sent, page by page, to the printer. Endpoint Prevent finds a violation on page three and stops the file from being printed at that point. Pages one and two have already printed. Pages three through ten are not printed. Endpoint Prevent sends an incident to the Endpoint Server containing file information and the matching text.

---

**Note:** The text in the cover page of a fax is not monitored.

---

The incident snapshot contains information regarding which endpoint computer sent the violating file, the violating file, and the printer name and the printer type. The printer type is either a locally connected printer, a shared printer, a network printer, or if the Print to file option has been selected.

See [“Setting report preferences”](#) on page 747.

See [“About Endpoint Prevent monitoring”](#) on page 1052.

## About clipboard monitoring

Endpoint Prevent stops users from copying and pasting sensitive data from one application to another by the Windows Clipboard. Endpoint Prevent only works on the Windows Clipboard and cannot prevent the Clipboard from transferring sensitive data between the same application.

For example, if a user copies sensitive information from a Word document and paste 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 747.

See [“About Endpoint Prevent monitoring”](#) on page 1052.

## About application monitoring

Application monitoring lets you monitor third-party applications for IM, email, or HTTP/S clients. By default, Symantec Data Loss Prevention only monitors first-party applications such as AIM, Microsoft Outlook, or Mozilla Firefox. Examples of third-party applications include Skype, Mozilla Thunderbird, or Google Chrome. Any application that is not specifically monitored by Symantec Data Loss Prevention must be added to the Application Monitoring page before Symantec Data Loss Prevention can begin monitoring. For example, if your company uses Mozilla Thunderbird, you must to add Thunderbird to the Application Monitoring page. You need to add the application because Mozilla Thunderbird is not monitored by default. After Mozilla Thunderbird is added, Symantec Data Loss Prevention monitors the application as it sends email messages through the network.

Additionally, you can configure global changes to default applications. 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 fingerprinting page. The applications on this page are only the applications that you want to modify for network, print/fax, Clipboard, or file system monitoring.

See [“About application monitoring”](#) on page 1131.

## About network share monitoring

Network share monitoring lets you prevent sensitive files from transferring between a network share and an endpoint computer.

For example, you have a local drive labeled c: drive. You also have a remote network share labeled g: drive. You can create a policy that blocks sensitive data from being copied from the c: drive to the g: drive. You can also prevent sensitive data transferring from the g: drive to the c: drive. Any Endpoint response rule is applicable to network share monitoring. For network share monitoring, Endpoint Protect only prevents sensitive data that transfers directly through Windows Explorer. Other types of network share access are not monitored. Other types of network share access include: FTP transfers, third-party applications, or copy/paste applications. These other types of network file share access are monitored by other detection features of Symantec Data Loss Prevention.

See [“About Endpoint Prevent monitoring”](#) on page 1052.

## 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
- CD/DVD
- Print/Fax
- Network Share
- Clipboard
- Application Monitoring

Endpoint Prevent lets you block network violations regardless of whether the endpoint computer 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 computer 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 1052.

## About Endpoint Discover monitoring

Endpoint Discover scans the local hard drive of endpoint computers to find any currently existing files that violate your policies. Endpoint Discover scans all fixed hard drives on your endpoint computers. For example, if your computer has two physical hard drives that are mounted to it, c: and e: and an external hard drive, f:, Endpoint Discover scans all three hard drives for those files that violate your policies. Endpoint Discover does not scan those drives that are mounted through a network or removable media such as flash drives or SD cards.

The Symantec DLP Agent can only perform DCM scans locally for Endpoint Discover. For all other types of scans, the Symantec DLP Agent sends the text of the files to the Endpoint Server for analysis. This design means that EDM and IDM detection must be done on the Endpoint Server.

For example, you set up an Endpoint Discover scan to examine all of the c: drives of all of your endpoint computers. The policy that is associated with the scan contains DCM content (keywords) as well as IDM components (credit card numbers). As the Endpoint Discover examines the c: drive, it automatically analyzes each file for the keywords. If it detects a file that potentially matches the indexed list of credit card numbers, it sends the file to the Endpoint Server for analysis.

To start or stop the scan, the Symantec DLP Agent must be connected to the Endpoint Server. If the Symantec DLP Agent is not connected to the Endpoint Server, the scan starts when it reconnects with the Endpoint Server. A scan is only complete when all of the endpoint computers have completed the scan. If one endpoint computer is disconnected from the Endpoint Server, the scan cannot complete until that endpoint computer reconnects to the Endpoint Server. If an endpoint computer is disconnected after a scan has started, the endpoint computer continues the scan. 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 size limit is reduced. The scan waits until the endpoint computer reconnects to the Endpoint Server and the Agent Store is cleared.

See [“About the Symantec DLP Agent”](#) on page 1052.

By default, the Symantec DLP Agent scans most of the files on the endpoint computer while the computer active. However, if the Symantec DLP Agent finds a file that requires a large amount of bandwidth to scan, the file is not scanned until the endpoint computer is idle. By waiting until the endpoint computer is idle, the Symantec DLP Agent uses less CPU bandwidth while users are active on the computer. You can configure how the Symantec DLP Agent defines the endpoint computer as idle. You can configure the Symantec DLP Agent so that it does not scan the endpoint computer at all while the computer is active.

See [“Advanced agent settings”](#) on page 204.

Incidents that are created for Endpoint Discover violations are sent to the Incidents section of the Enforce Server. Incidents appear under the Discover tab of the Incidents section. Incidents are marked with an Endpoint-specific icon. You cannot automatically remediate Endpoint Discover incidents. If you want to perform any type of remediation on the incidents that are recorded in Endpoint Discover, you must manually remediate the incidents.

See [“About Endpoint reports”](#) on page 1066.

## About targeted Endpoint Discover scans

You can target all of the endpoint computers that are connected to a specific Endpoint Server. Or, you can target individual endpoint computers for Endpoint Discover scans. Based on a set of filters that you specify, individual Symantec DLP Agents that are attached to the Endpoint Server start the scan. When the Endpoint Server begins the scan, the scan information is distributed to all of the associated Symantec DLP Agents. The Symantec DLP Agents analyze the scan with the scan filters.

If a Symantec 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 Symantec DLP Agents based on the scan filters, those Symantec DLP Agents cannot be scanned until the first scan is complete.

See [“Setting up scanning of an Endpoint Discover target”](#) on page 1071.

## About policies for endpoint computers

Symantec Data Loss Prevention uses a two-tiered detection architecture to analyze activity on endpoint computers. It performs detection directly on Symantec DLP Agents or detection occurs 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) only. 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.

Two-tiered detection has implications for the kinds of detection rules and response rules you can combine in a policy and use on endpoint computers. It also has implications for the optimization of system usage and performance of Symantec

Data Loss Prevention on endpoint computers. As you create the policies that apply to endpoint computers, 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, IDM, 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.

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 Sender 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. When you set up the compound rule in this way, the Symantec 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, IDM, or DGM 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 content to an Endpoint Server for analysis, the Symantec DLP Agent sends either text data or binary data according to detection requirements. Whenever possible, Symantec 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, Symantec DLP Agents must send binary data to the Endpoint Server. In this case, make sure that your network can handle the increased traffic between Symantec 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 Symantec DLP Agent detection rule triggers the response.

See [Table 63-2](#) on page 1062.

**Table 63-2** Incompatible detection rules and response rules

Do not combine these server-based detection rules...	...with these Endpoint Prevent response rules.
<ul style="list-style-type: none"> <li>■ Content Matches Exact Data (EDM)</li> <li>■ Content Matches Document Signature (IDM)</li> <li>■ Sender/User Matches Directory (DGM)</li> <li>■ Recipient Matches Directory (DGM)</li> </ul>	<ul style="list-style-type: none"> <li>■ Endpoint: Block</li> <li>■ Endpoint: Notify</li> <li>■ Endpoint: User Cancel</li> </ul>

## About policy creation for Endpoint Prevent

Policies for Endpoint Prevent differ from Network Prevent policies.

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 on 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 files 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 endpoint computers”](#) on page 1060.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## 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 computer. For example, Email/STMP, HTTP/HTTPS, CD/DVD, FTP, 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

To gain a better understanding of how Endpoint Prevent policies work, the following examples describe specific Endpoint Prevent situations. The described situations are not the only possibilities and are only shown as examples.

See [“Implementing policies”](#) on page 317.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About Endpoint Block

You can create a policy to restrict any data from transferring from the endpoint computer. 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 [“Implementing policies”](#) on page 317.

You want to ensure that this policy is used across all endpoint computers. 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 computer. 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.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## 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 computer. 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.

See [“About policies for endpoint computers”](#) on page 1060.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## **About Endpoint User Cancel**

You can create a response rule that lets endpoint computer 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 731.

See [“About policies for endpoint computers”](#) on page 1060.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## 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 [“Introduction to policy detection”](#) on page 281.

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 endpoint computers. 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 745.

See [“How to implement Endpoint Prevent”](#) on page 1075.

See [“How to implement Endpoint Discover”](#) on page 1067.

# Implementing Endpoint Discover

This chapter includes the following topics:

- [How to implement Endpoint Discover](#)

## How to implement Endpoint Discover

When you implement Endpoint Discover, you need to follow a specific set of tasks. These tasks are similar to Network Discover, but not identical. To implement Endpoint Discover, you must complete the following configuration tasks:

**Table 64-1** Implementing Endpoint Discover

Phase	Action	Description
Step 1	Install the Symantec Management Console (Optional).	See <a href="#">“About the Symantec Management Console”</a> on page 1097.
Step 3	Set the Endpoint Location.	See <a href="#">“Setting the endpoint location”</a> on page 1076.
Step 4	Modify the Endpoint Server configuration.	See <a href="#">“Server configuration–basic”</a> on page 152.
Step 5	Create a policy group.	See <a href="#">“Creating a policy group for Endpoint Discover”</a> on page 1068.
Step 6	Create a policy.	See <a href="#">“Creating a policy for Endpoint Discover”</a> on page 1068.
Step 7	Create an Endpoint Discover target.	See <a href="#">“Setting up scanning of an Endpoint Discover target”</a> on page 1071.

**Table 64-1** Implementing Endpoint Discover (*continued*)

Phase	Action	Description
<b>Step 8</b>	Install the Symantec DLP Agent.	See <a href="#">“About Symantec DLP Agent Installation”</a> on page 1102.
<b>Step 9</b>	Configure reports.	See <a href="#">“About Symantec Data Loss Prevention reports”</a> on page 745.

Each of these steps is necessary to correctly implement Endpoint Discover. For more information on any subject of implementing Endpoint Discover, see the online Help.

## 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 on each endpoint computer that is connected to the Endpoint Server. After you have created the policy group, you can assign specific policies to the policy group.

### To create a policy group

- 1 Go to **Administration > Settings > Policy Groups**.
- 2 On the Policy Group List screen that appears, click **Add Policy Group**.
- 3 Enter a policy-group name (of up to 256 characters) and a description. Choose an informative name, since other users must access it when choosing which policy group(s) to associate with roles, policies, and Endpoint Discover targets.
- 4 Choose the detection server to assign to this policy group. You can assign the policy group to all detection server or to individual servers. Note that Symantec Data Loss Prevention automatically assigns all policy groups to all Endpoint Discover Servers. This feature gives you the ability to assign policy groups to individual Endpoint Discover targets.
- 5 Click **Save**.

See [“How to implement Endpoint Discover”](#) on page 1067.

## 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. The Symantec DLP Agent sends files to the Endpoint Server for analysis. IDM, EDM,

and DGM policies are all performed on the Endpoint Server. The Symantec DLP Agent sends the opened files from the endpoint computer to the Endpoint Server for analysis.

See [“About policies for endpoint computers”](#) on page 1060.

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 Symantec 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.

For example, assume that you want to create an Endpoint Discover policy to find files with any identification numbers that begin with 1357. You have a list of all of the numbers that can start with 1357. The list was uploaded to the Symantec Data Loss Prevention system under the name EDM\_m1. Symantec Data Loss Prevention creates a policy that discovers any files on the endpoint that contain any of this sensitive data.

#### To create a policy for Endpoint Discover

- 1 Go to **Policy > Policy List** on the Enforce Server.
- 2 Click **New Policy**.
- 3 Select **Add a blank policy**.
- 4 Enter **1357 identifier** in the Name field.
- 5 Add **Discover any identifiers starting with 1357** in the Description field of the new policy.
- 6 Select the policy group you want associated with this policy from the drop-down menu.

For this example, use **EP eDAR**.

After you create the policy, you must add rules to the policy.

See [“Adding a rule for Endpoint Discover”](#) on page 1069.

See [“How to implement Endpoint Discover”](#) on page 1067.

## 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 1068.

### To add a rule to a policy

- 1 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 **EDM m1** from the drop-down menu.  
This procedure links the previously created list to the rule.
- 4 Click **Next**.

See [“How to implement Endpoint Discover”](#) on page 1067.

## About Endpoint Quarantine

You can create an automated response rule that allows Endpoint Discover policies 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 computer users that the file contained confidential information and was quarantined. 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.

Endpoint quarantine response rules are only applicable to Endpoint Discover.

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 computer 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 will receive an error message. The error states that the policy is incompatible with the Endpoint response rules.

See [“About policies for endpoint computers”](#) on page 1060.

See [“How to implement Endpoint Prevent”](#) on page 1075.

See [“Configuring the Endpoint Discover: Quarantine File action”](#) on page 722.

## Setting up scanning of an Endpoint Discover target

An Endpoint Discover target is the actual location that the Symantec DLP Agent scans. It corresponds to the target hard drive, folders, or endpoint computers that Endpoint Discover examines to find violations of your policies. For example, the c: drive or the My Documents folder in Windows. Endpoint Discover targets can scan any fixed drive that is associated with the endpoint computer, however, it cannot scan removable drives. You can also specify filters to determine which endpoint computers you monitor. This filtering is called targeted Endpoint Discover scanning.

**Table 64-2**      Setting up an Endpoint Discover target

Step	Description	Action
Step 1	Click <b>Policies &gt; Discover Scanning &gt; Discover Targets</b> to configure a new Endpoint Discover target.	See <a href="#">“Adding a new Network Discover target”</a> on page 850.
Step 2	Perform any additional filter configurations for targeted Endpoint Discover scanning.	See <a href="#">“Configuration options for endpoint targets”</a> on page 1072.

**Note:** You cannot schedule Endpoint Discover targets. Each scan must be started manually. You can also manually stop the scan or allow it to complete. You cannot pause an Endpoint Discover scan.

See [“How to implement Endpoint Discover”](#) on page 1067.

### About Endpoint Discover target filters

Endpoint Discover target filters affect how Endpoint Discover interacts with your endpoint computers. Endpoint Discover target filters let you specify the following:

- Limit or specify exactly what type of files you scan.
- The areas within the target you want to scan.
- The subset of endpoint computers 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 [“Setting up scanning of an Endpoint Discover target”](#) on page 1071.

See [“Configuration options for endpoint targets”](#) on page 1072.

See [“How to implement Endpoint Discover”](#) on page 1067.

## Configuration options for endpoint targets

Endpoint Discover targets do not let you specify an Endpoint Server. Endpoint targets are associated with Symantec DLP Agents and are dedicated to a specific Endpoint Server.

Only one Endpoint Discover scan can run at a time. Any endpoint computers that the targeted Endpoint Discover scan excludes display a **Not Participating** status and are not scanned.

You can specify filters to determine which endpoint computers you monitor. This filtering is called Targeted Endpoint Discover scanning.

Name	See <a href="#">“Configuring the required fields for Network Discover targets”</a> on page 857.
Policy Groups	
Servers	
Include Filters	See <a href="#">“Setting up Discover filters to include or exclude items from the scan”</a> on page 861.
Exclude Filters	See <a href="#">“Setting up Discover filters to include or exclude items from the scan”</a> on page 861.
Size Filters	See <a href="#">“Filtering Discover targets by item size”</a> on page 864.
Date Filters	See <a href="#">“Filtering Discover targets by date last accessed or modified”</a> on page 865.

The include and exclude filters are designed so that you can filter the following:

- Files
- File folders
- IP addresses
- Computer names
- WINS names

For example, you can include the following filters under the Include filters sections:

```
*.doc, $Documents$, >*.symantec.com, >192.168.32.0/8, >EDT*
```

The targeted 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 endpoint computers in the .symantec.com domain
- All computers on the 192.168.32.0/8 network
- Any endpoint computers with the WINS name EDT

Separate multiple filters with commas.

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.

Structurally, the filters are Boolean in that similar filters are applied using the OR expression and then combined with other filters using the AND expression. Using the example, the Symantec DLP Agent scans

```
*.doc OR $Documents$* AND >*.symantec.com OR >192.168.32.0/8.
```

The \*.doc and \$Documents\$ filters use the OR expression because they are file or file path filters. The >.symantec.com and > 192.168.32.0/8 filters use the OR expression because they are IP filters and are similar to each other. The two sets of similar filters combine using the AND expression.



# Implementing Endpoint Prevent

This chapter includes the following topics:

- [How to implement Endpoint Prevent](#)

## How to implement Endpoint Prevent

Endpoint Prevent monitors each endpoint computer for data that is moved from one place to another. If Endpoint Prevent detects a violation, it blocks the data from being transferred. Or, it 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 65-1** Implementation steps

Step	Action	Action
Step 1	Install the Symantec Management Console (Optional)	See <a href="#">“About the Symantec Management Console”</a> on page 1097.
Step 2	Install the Symantec DLP Agent	See <a href="#">“About Symantec DLP Agent Installation”</a> on page 1102.
Step 3	Set the Endpoint Location	See <a href="#">“Setting the endpoint location”</a> on page 1076.

**Table 65-1** Implementation steps (*continued*)

Step	Action	Action
<b>Step 4</b>	Create endpoint agent configurations	See <a href="#">“About agent configurations”</a> on page 1081.
<b>Step 5</b>	Add an Endpoint Server	See <a href="#">“Adding a detection server”</a> on page 166.
<b>Step 6</b>	Create an Endpoint policy	See <a href="#">“Implementing policies”</a> on page 317.
<b>Step 7</b>	Create Endpoint response rules	See <a href="#">“About policy creation for Endpoint Prevent”</a> on page 1062.
<b>Step 8</b>	Configure reports	See <a href="#">“About Symantec Data Loss Prevention reports”</a> on page 745.

Each of these steps are necessary to correctly implement Endpoint Prevent. For more information on any subject of implementing Endpoint Prevent, please see the online Help.

See [“About implementing synchronized Directory Group Matching”](#) on page 511.

## Setting the endpoint location

The endpoint location is used to define how Symantec Data Loss Prevention determines whether or not the endpoint computer is connected to the corporate network. You can specify if you want the Endpoint Server to automatically detect if the endpoint computer is on the corporate network. Or, you can specify a list of domain names or IP addresses to use to determine if the endpoint computer is connected to the network.

With automatic endpoint location determination, a computer is considered connected to the network if the Symantec DLP Agent can connect to the Endpoint Server. If the Symantec DLP Agent cannot connect to the Endpoint Server, the endpoint computer is judged to be disconnected from the corporate network. With manual endpoint location determination, you must first input a range of domain names or IP addresses. The Symantec DLP Agent then uses this information to determine if the endpoint computer is connected to the corporate network. If a range of domain names is configured, the Symantec 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 Symantec 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 computer 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 1052.

### To set the Endpoint Location setting

- 1 Go to **System > Agent > Endpoint Location**. The current endpoint location settings are displayed. By default, the endpoint location determination is set to **Automatic**.
- 2 Click **Configure**.
- 3 Select **Automatically** or **Manually** to specify the determination method.
- 4 If you select **Manually**, enter a list of domain names or IP addresses in the correct field. Enter only one domain name or IP address per line.
- 5 Click **Save**.

The changes take effect immediately.

See [“How to implement Endpoint Prevent”](#) on page 1075.

See [“Endpoint Server–basic configuration”](#) on page 163.

## 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 computer. A locale refers to the system locale setting in the operating system of the endpoint computer.

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 computer and a Vietnamese-locale endpoint computer. 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 computer, that language cannot be considered the default language. The endpoint computer 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 computer, regardless of the system locale of the endpoint computers.

See [“Advanced agent settings”](#) on page 204.

---

**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 1078.

## 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 1077.

### Setting a localized response rule

- 1 Create the response rule normally.  
See [“Configuring response rules”](#) on page 697.
- 2 Click the **Add Language** link.
- 3 Select the language that you want to use.  
If you want to specify an unsupported language as the default language, select **Other**.
- 4 Enter text in the display fields and the justification fields using the designated language.
- 5 Click **Save**.



# Working with agent configurations

This chapter includes the following topics:

- [About agent configurations](#)
- [Adding agent configurations](#)
- [Applying agent configurations to an Endpoint Server](#)

## About agent configurations

The Agent Configuration page on the Enforce Server administration console lets you create configurations that you can either apply to Endpoint Servers.

You can apply these configurations to individual Symantec DLP Agents through the Symantec Management Console (SMC).

Each configuration contains configuration options for your Endpoint Servers or agents. These configuration options determine the types of detection that occurs on the endpoint computer. You can also specify filters and resource consumption limits using agent configurations. 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.

See [“Adding agent configurations”](#) on page 1082.

Endpoint Servers can only use one configuration at a time. You cannot associate more than one configuration to an Endpoint Server at a time.

You can assign agent configurations either through the Symantec Management Console (SMC) or through the Enforce Server administration console. You cannot

use the SMC to create new agent configurations. You can only create configurations in the Enforce Server administration console. If you assign the agent configurations through the SMC, you can assign the configurations directly to the agents. If you assign the agents through the Enforce Server, you can only assign the agent configurations to Endpoint Servers.

You can also clone agent configurations.

See [“About cloning agent configurations”](#) on page 1082.

See [“Applying agent configurations to an Endpoint Server”](#) on page 1087.

## 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.

Click **Add Configuration** to create new agent configurations.

## 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 to monitor.

Field	Description
<b>Destinations</b>	Select the destinations to be monitored. Destinations are physical aspects of the endpoint computer such as CD/DVD drives, USB-connected devices, printers, and so on.
<b>Email</b>	Select email applications to be monitored.
<b>Web</b>	Select Web applications to be monitored. HTTPS monitoring is only supported for Firefox and Internet Explorer browsers.
<b>Instant Messaging</b>	Select instant messaging applications to be monitored.
<b>Applications</b>	Select to add application file access monitoring. See <a href="#">“About application monitoring”</a> on page 1131.
<b>Network Shares</b>	Select to monitor network shares. You can monitor files that are transferred to or from your local drive and a network share.

- **Filter by File Properties** section. Create and edit monitoring filters. 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.
  - 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.
- **Default File Filter Action** section. Choose either **Monitor** or **Ignore** to specify what to do with the files that do not match any of the filters.
- **Filter by Network Properties** section. 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_entries := protocol_filter_entry  
                                [; protocol_filter_multiple_entries]  
protocol_filter_entry            := +|- , destination_subnet_description,  
                                source_subnet_description  
destination_subnet_description   := subnet_description  
source_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.

---

**Note:** The Domain filters need to be applied separately for HTTP and HTTPS. To add filters for any Web site 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 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 Symantec DLP Agent can use to send data to the Endpoint Server. 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.
- **Resource Consumption on the Endpoint Host** section. Use this section to set the maximum disk space that is used by the Agent Store on each Endpoint system for storing incidents. You can specify a percentage of the hard drive, or a particular size in the specified unit of measure (Bytes, KB, MB, or GB).

Click the appropriate radio button to choose either a percentage of disk space or an absolute storage limit. Then enter the amount in the corresponding box. For absolute size, choose the unit of measurement from the drop-down list. See [“About the Symantec DLP Agent”](#) on page 1052.

- **Resource Consumption for Endpoint Discover Scans** section. Use this section to limit the effect of Discover scans on Endpoint systems:

Field	Description
<b>Long-Term Average CPU Usage</b>	<p>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.</p> <p><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.</p>
<b>Minimum Battery Life Remaining</b>	<p>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.</p>

- **File Recovery Area Location** section. Specify file recovery parameters. File recovery location is where copies of the sensitive data that the Symantec 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
<b>File Recovery Area Location</b>	Specify the path to the file recovery directory. The default is %TMP\RecoveredFiles.
<b>Time To Expiration</b>	Specify the amount of time before files are automatically deleted from the file recovery folder.

See [“About Symantec Data Loss Prevention administration”](#) on page 45.

See [“Server configuration—basic”](#) on page 152.

See [“Server controls”](#) on page 151.

**Advanced Agent Settings** tab.

You can also specify advanced settings for the agents. These settings affect how the Symantec DLP Agent process information, detect violations, and performs on your endpoint computers.

Use caution when modifying advanced agent settings. Contact Symantec Support before changing any of the advanced settings.

See [“Advanced agent settings”](#) on page 204.

Consult Symantec Data Loss Prevention online Help for information about advanced agent settings.

---

**Note:** If you modify an existing agent configuration, clicking the **Save and Apply** button applies the changes to all of the Endpoint Servers associated with the configuration. If you create a new configuration, the configuration is saved and you can apply it on the **Edit agent configuration** page.

---

See [“About agent configurations”](#) on page 1081.

See [“Applying agent configurations to an Endpoint Server”](#) on page 1087.

## Applying agent configurations to an Endpoint Server

You can apply any agent configuration to any Endpoint Server that is connected to the Enforce Server administration console. You can assign only one agent configuration to an Endpoint Server at a time. However, you can assign configurations to multiple Endpoint Servers at one time. Use the Apply

Configuration page to assign agent configuration entities to all of your Endpoint Servers at one time.

If you use the Symantec Management Console to apply agent configuration, you can apply your configurations directly to your agents. After the agents receive the configurations, they are associated with specific Endpoint Servers.

See the *Symantec Management Console online Help* for more information.

See [“About agent configurations”](#) on page 1081.

#### **Applying an agent configuration to an Endpoint Server**

- 1** Click the **Apply Configuration** button from the main Agent configuration page.
- 2** Select the Endpoint Servers that you want.
- 3** Select the agent configuration you want from the drop-down menu.
- 4** Click **Apply and Update**.

If you want to make edits to your agent configuration entities and apply those changes immediately to your associated Endpoint Servers, you can. Click the **Save and Apply** button from the Editing Configuration page.

See [“Adding agent configurations”](#) on page 1082.

# Working with Endpoint FlexResponse

This chapter includes the following topics:

- [About Endpoint FlexResponse](#)
- [Deploying Endpoint FlexResponse](#)
- [Deploying Endpoint FlexResponse plug-ins on endpoint computers](#)
- [Installing Endpoint FlexResponse plug-ins using a silent installation process](#)
- [About the Endpoint FlexResponse utility](#)
- [Loading Endpoint FlexResponse plug-ins using the Endpoint FlexResponse utility](#)
- [Enabling Endpoint FlexResponse on the Enforce Server](#)
- [Uninstalling Endpoint FlexResponse plug-ins using the FlexResponse utility](#)
- [Retrieving Endpoint FlexResponse plug-ins from a specific endpoint computer](#)
- [Retrieving a list of Endpoint FlexResponse plug-ins from an endpoint computer](#)

## About Endpoint FlexResponse

Endpoint FlexResponse provides you with additional flexibility to remediate incidents. When you first install Endpoint Prevent, you have a fixed set of response rule actions available to use. But by installing an Endpoint FlexResponse plug-in (developed by Symantec or by Symantec partners), you can remediate incidents in a wide variety of ways including encryption, applying digital rights management, or redacting confidential information. For example, you can create an Endpoint

FlexResponse rule that automatically protects files by integrating with a Digital Rights Management Service.

You can use Endpoint FlexResponse rules on the following types of endpoint destinations and protocols:

- Endpoint Discover
- Hard drive monitoring
- USB-connected devices
- SMTP
- HTTP(S)

After you have installed the Endpoint FlexResponse plug-in, you can add it as a response rule action in your policy.

---

**Note:** Endpoint FlexResponse rules are only applicable to automatic response rules. You cannot create Endpoint FlexResponse rule actions for manual remediation policies.

---

You can create credentials for the Endpoint FlexResponse plug-ins. These credentials can be Endpoint-specific, or they can apply to all of your detection servers. Credentials let you assign specific users access to the remediated data.

See [“Configuring endpoint credentials”](#) on page 100.

See [“Adding a new response rule”](#) on page 697.

See [“Configuring the Endpoint: FlexResponse action”](#) on page 721.

## Deploying Endpoint FlexResponse

Follow the steps provided here to deploy Endpoint FlexResponse plug-ins.

**Table 67-1** Deploying Endpoint FlexResponse

Step	Action	Description
Step 1	Obtain the Endpoint FlexResponse plug-in.	Contact your Symantec Sales representative.
Step 2	Configure any Endpoint credentials on the Enforce Server.	See <a href="#">“Configuring endpoint credentials”</a> on page 100.  This step is optional.

**Table 67-1** Deploying Endpoint FlexResponse (*continued*)

Step	Action	Description
Step 3	Deploy the plug-in to your endpoint computers using the FlexResponse utility and third-party systems management software (SMS).	See <a href="#">“Deploying Endpoint FlexResponse plug-ins on endpoint computers”</a> on page 1091.
Step 4	Enable Endpoint FlexResponse actions on your Enforce Server.	See <a href="#">“Enabling Endpoint FlexResponse on the Enforce Server”</a> on page 1094.
Step 5	Add Endpoint FlexResponse actions to your policies.	See <a href="#">“Adding a new response rule”</a> on page 697.

## Deploying Endpoint FlexResponse plug-ins on endpoint computers

You can deploy Endpoint FlexResponse plug-ins to endpoint computers only after you have installed the Symantec DLP Agents.

See the *Symantec Data Loss Prevention Installation Guide* for information on how to install the agents.

Endpoint FlexResponse plug-ins must be installed on your endpoint computers. Endpoint FlexResponse response rules cannot operate if the plug-in is not installed on each of your endpoint computers.

Use a silent installation method to install the Endpoint FlexResponse plug-in. Silent installation methods involve systems management software (SMS).

SMS applications are third-party applications that distribute software to all of your endpoint computers. Symantec highly recommends that you use an SMS application to install and deploy the Endpoint FlexResponse plug-ins. You may need to create SMS scripts to access the installation folder.

Installing the Endpoint FlexResponse plug-in is a two-part process:

- Install the Endpoint FlexResponse plug-in and the FlexResponse utility on your endpoint computers. See [“Installing Endpoint FlexResponse plug-ins using a silent installation process”](#) on page 1092.
- Load the Endpoint FlexResponse plug-in using the FlexResponse utility. See [“Loading Endpoint FlexResponse plug-ins using the Endpoint FlexResponse utility”](#) on page 1093.

# Installing Endpoint FlexResponse plug-ins using a silent installation process

Before you can deploy your Endpoint FlexResponse plug-in, the endpoint computers in your organization must first be able to access the physical plug-in .zip file.

You can either place the plug-in .zip file somewhere on a central network share, or you can install the file physically on each endpoint computer. If you use the central network share method, you must ensure that all of your endpoint computers can access the network share. Use the following procedure if you want to install the plug-in .zip file physically on each endpoint computer. This procedure only instructs you how to access the plug-in .zip file. After you access the file, you must deploy it.

See [“Loading Endpoint FlexResponse plug-ins using the Endpoint FlexResponse utility”](#) on page 1093.

See your individual SMS application documentation for more information on how to install using SMS.

## To install Endpoint FlexResponse plug-ins

- 1 In your systems management software package, specify the plug-in(s) that you want to install.
- 2 Specify the installation parameters such as the installation directory.  
Plug-ins can be installed anywhere on the endpoint computer because they are deployed to the correct Symantec DLP Agent database later.
- 3 Specify the `msiexec` properties.
- 4 Install the FlexResponse utility to all of your endpoint computers as well.  
The FlexResponse utility is only available through Symantec and Symantec partners.

See [“About the Endpoint FlexResponse utility”](#) on page 1092.

## About the Endpoint FlexResponse utility

The Endpoint FlexResponse utility manages Endpoint FlexResponse plug-ins.

The Endpoint FlexResponse utility is not part of the normal Symantec Data Loss Prevention download. The utility is only available through Symantec or Symantec partners.

The utility lets you perform the following actions:

**Table 67-2** Endpoint FlexResponse utility actions

Action	Description
Load plug-ins	Use the install command to load plug-ins on an endpoint computer.
Uninstall plug-ins	Use the uninstall command to uninstall plug-ins from an endpoint computer.
Retrieve installed plug-ins	Use the retrieve command to retrieve a specific plug-in that has already been installed on an endpoint computer. The plug-in appears as an editable text file in the Symantec DLP Agent installation directory.
See a list of installed plug-ins	Use the list command to retrieve a list of all plug-ins that are installed on a specific endpoint computer. The list is composed of only the names of the installed plug-ins.

The Endpoint FlexResponse utility must be run from the agent installation folder. By default, that directory is located at:

```
c:\Program Files\Manufacturer\Endpoint Agent\Tools\flrinst.exe
```

The name of the utility is flrinst.exe.

---

**Note:** Depending on your operating system, this path may not apply to your system.

---

Because the utility lets you retrieve and modify already installed plug-ins, set your SMS application to remove the utility after you have used it. Removing the utility prevents any unauthorized modification or uninstallation of your plug-ins.

## Loading Endpoint FlexResponse plug-ins using the Endpoint FlexResponse utility

---

**Note:** Endpoint FlexResponse plug-ins must be in a .zip package format. You cannot deploy the plug-ins if they are in any other format.

---

You must use the utility from the Symantec DLP Agent installation tools directory.

### To load Endpoint FlexResponse plug-ins

- 1 From a command window, navigate to the Symantec DLP Agent installation tools directory.

```
<Agent installation directory>\Tools\flrinst.exe
```

- 2 Enter the following command:

```
-op=install -package=<Plug-in name>
```

where *<Plug-in name>* is the specific name of the plug-in .zip file.

- 3 Repeat step 2 until you have loaded all of your plug-ins.
- 4 Using your SMS application, remove the utility from your endpoint computers.

See [“Deploying Endpoint FlexResponse”](#) on page 1090.

See [“About the Endpoint FlexResponse utility”](#) on page 1092.

## 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. Enable Endpoint FlexResponse functionality through the Advanced Agent Settings.

### To enable Endpoint FlexResponse functionality

- 1 Go to: **System > Agents > Agent Configuration** and open the configuration for editing.
- 2 Click the **Advanced Agents Settings** tab.
- 3 Find the `PostProcessor.ENABLE_FLEXRESPONSE.int` setting.
- 4 Change the setting to **1**.
- 5 Click **Save and Apply**.

See [“Adding a new response rule”](#) on page 697.

See [“Deploying Endpoint FlexResponse”](#) on page 1090.

# Uninstalling Endpoint FlexResponse plug-ins using the FlexResponse utility

Use the following procedure to uninstall Endpoint FlexResponse plug-ins from your endpoint computers:

## To uninstall Endpoint FlexResponse plug-ins from endpoint computers

- 1 Using a command prompt window, navigate to the Symantec DLP Agent installation tools directory.

```
<Agent installation directory>\Tools\flrinst.exe
```

- 2 Enter the following command:

```
-op=uninstall -package=<Plug-in name>
```

where *<Plug-in name>* is the full path where the plug-in resides and the specific name of the plug-in .zip file.

- 3 Repeat step 2 until you have uninstalled all of the plug-ins.

# Retrieving Endpoint FlexResponse plug-ins from a specific endpoint computer

Use the following procedure to retrieve a specific plug-in from an endpoint computer. You can only use the retrieve function on a single endpoint computer at a time. The plug-in appears in the Symantec DLP Agent installation directory as a .zip file. Inside the .zip file is the plug-in in a .txt format. You can make edits to the plug-in in the .txt file. If you do make edits, you must re-deploy the plug-in to the endpoint computer before the edits take effect. Modified plug-ins only affect the individual endpoint computers where they were modified.

## To retrieve an Endpoint FlexResponse plug-in from a specific endpoint computer

- 1 On the endpoint computer, open a command prompt window.
- 2 Navigate to the Symantec DLP Agent installation tools directory:

```
<Agent installation directory>\Tools\flrinst.exe
```

- 3 Enter the following command:

```
-op=retrieve -package=<Plug-in name>
```

where *<Plug-in name>* is the specific name of the plug-in .zip file.

- 4 Look in the Symantec DLP Agent installation directory for a .txt file that contains the same name as the plug-in.

## Retrieving a list of Endpoint FlexResponse plug-ins from an endpoint computer

Use the following procedure to retrieve a list of plug-ins that have been installed on a specific endpoint computer. You can only use the list function on individual endpoint computers. You cannot use the list function on a set of endpoint computers.

The list of endpoint computers contains only the name of the plug-in package. The list does not contain any type of description about the plug-ins. It is recommended 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 computer

- 1 On the endpoint computer, open a command prompt window.
- 2 Navigate to the Symantec DLP Agent installation tools directory:

```
<Agent installation directory>\Tools\flrinst.exe
```

- 3 Enter the following command:

```
-op=list
```

The list of installed Endpoint FlexResponse plug-ins appears in the Command prompt window.

# Implementing Symantec DLP Agents

This chapter includes the following topics:

- [About the Symantec Management Console](#)
- [About Symantec DLP Agent Installation](#)

## About the Symantec Management Console

The Symantec Management Console (SMC) provides a centralized way for you to manage your Symantec DLP Agent installations, upgrades, and uninstalls. Using SMC, you can find all of the endpoint computers in your organization and add them to the SMC for management. You can also create your own organizational structure or use a predefined structure such as Active Directory (AD). The Symantec Management Console contains troubleshooting tools that let you investigate your Symantec DLP Agents in case there is a problem.

---

**Note:** Installing and using the Symantec Management Console with Symantec Data Loss Prevention is optional. You do not need to use the Symantec Management Console to protect your data. However, the Symantec Management Console offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention.

---

Symantec Management Console uses single sign-on (SSO) technology. You do not have to maintain separate credentials for Symantec Data Loss Prevention and Symantec Management Console.

For more information, see the *Symantec Management Platform Installation Guide*. See [“How to implement Endpoint Prevent”](#) on page 1075.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“About Symantec Management Console agent tasks”](#) on page 1101.

## Cloning advertisements and programs

If you have more than one Endpoint Server, clone your advertisements and programs. This procedure lets you install, upgrade, or uninstall the Symantec DLP Agent and the Symantec Management Agent across each of your Endpoint Servers. Cloning advertisements and programs let you copy your specific installation parameters for each Endpoint Server. Name the cloned advertisements in a similar fashion as your programs.

For example, you create a program and advertisement to install the Symantec DLP Agent on an Endpoint Server named EndpointServer1. You also have an Endpoint Server named EndpointServer2. You should clone the program and advertisement that you used for EndpointServer1 and rename the clones as EndpointServer2. All of the installation parameters you specified for EndpointServer1 are maintained for EndpointServer2. You must change the destination directory for your second Endpoint Server.

### Cloning advertisements and programs

- 1 In the Symantec Management Console, find the advertisement or program that you want to clone.
- 2 Right-click the advertisement and then select **Clone**.
- 3 Enter the name for the cloned advertisement or Program.
- 4 Click **OK**.
- 5 Adjust the destination settings and any other parameters that you want.

For more information about the Symantec Management Console and what you can do with it, see the *Symantec Management Platform Administration Guide*.

See [“About the Symantec Management Console”](#) on page 1097.

## Using computer discovery

Computer discovery lets you find and register all of your endpoint computers with Symantec Management Console. This feature lets you see how many endpoint computers you have on your network and how many Symantec DLP Agents you need to install. You can use either Active Directory to add endpoint computers, or you can browse through different domains to specify the network that you want. Any endpoint computers in the network that you specify are eligible for installation. You can also manually add computers to your network.

### Using computer discovery

- 1 Under the **System** section of the DLP Portal page, click the **Discover Computers** link.
- 2 Select either the **Active Directory Import** option or the **Domain Browse** option.
- 3 For **Domain Browse**, add the domain you want either by entering the domain name or browsing for it in the **Domain Picker**. Select the schedule that you want the discover computer tool to update the list of endpoint computers and click **Save Changes**.
- 4 For Active Directory Import, select the resource import rules that you want to use to discover your endpoint computers and select a directory synchronization schedule. Click **Save Changes**.

See [“About the Symantec Management Console”](#) on page 1097.

## Installing the Symantec Management Agent

You must install the Symantec Management Agent before you install the Symantec DLP Agent. The Symantec Management Agent and the Symantec DLP Agent run concurrently on your endpoint computers. The Symantec Management Agent lets you deploy the Symantec DLP Agent. It also lets you use a number of troubleshooting agent tasks.

---

**Note:** In Symantec Data Loss Prevention v11.x, SMP v7.0 and SMP v7.1 are supported.

---

### Installing the Symantec Management Agent

- 1 From the DLP Portal page click the **Install Symantec Management Agent** link.
- 2 Click the **Select Computers** option and select the specific endpoint computers where you want the Symantec Management Agent installed.
- 3 Click the **Install Symantec Management Agent** option.
- 4 Click **Proceed with Install**. The installation starts immediately.

---

**Note:** If you want to set the installation on a schedule, click **Installation Settings** and modify the settings in the pop-up window.

---

After you have installed the Symantec Management Agent, you can install the Symantec DLP Agent.

## About Symantec Management Console reporting

You can view reports and "Gets" status about the installation updates and deployment updates for both agents. The reports are contained on the portal page of the Symantec Management Console application. View the reports by going to: **Reports > DLP IC** in the left-hand navigation pane.

The reports display:

- The number of endpoint computers in your network that are installed with the Symantec DLP Agent.
- Status updates for how many endpoint computers remain without the Symantec DLP Agent.
- The number of endpoint computer that have the Symantec DLP Agent installed, but not registered with the Symantec Management Console.
- The percentage of the endpoint computers that are in each state.
- The status of the DLP print screen states on the endpoint computers. This status indicates whether or not the print screen functionality is disabled.
- The details of Symantec DLP Agent configuration statuses. This report indicates details about the agents and current configurations that are assigned to those agents.

Depending on the type of report you want, you can add filters to the report to see specific information.

System administrators can create their own reports through the Symantec Management Console.

For more information on reporting in the Symantec Management Console, see the *Symantec Management Platform User's Guide*.

You can also see different jobs and the status of those jobs that the Symantec Management Agent performs. The jobs and their status are divided into the following sections:

- Description
- Start Time
- Status

You can group these Symantec Management Agent jobs by status and you can search for specific jobs.

For more information, see the *Symantec Management Platform User's Guide*.

See "[About the Symantec Management Console](#)" on page 1097.

## About Symantec Management Console agent tasks

The Symantec Management Console comes with a number of tasks that let you troubleshoot the Symantec DLP Agent if there is a problem. The agent tasks consist of the following:

- **Start Agents**  
Selecting the Start agents task manually starts specific Symantec DLP Agents in your network.
- **Stop Agents**  
Selecting the Stop agents task stops specific Symantec DLP Agents in your network.
- **Restart Agents**  
Selecting the Restart Agents task restarts specific stopped Symantec DLP Agents in your network.
- **Kill Agents**  
Lets you kill the Symantec DLP Agent.
- **Change Endpoint Server**  
Lets you set specify the hostname and IP address of the current Endpoint Server. Also, you can specify secondary Endpoint Servers in case the primary one fails..
- **Set DLP Agent Configuration**  
Assigns Endpoint configurations to Symantec DLP Agents.  
See [“About agent configurations”](#) on page 1081.
- **Get Agent Configuration**  
Selecting the Get configuration task collects the configuration for the Symantec Management Agent. This information is stored in the path that is specified in the DLP IC Configuration page.
- **Toggle Print Screen**  
Turns print screen functionality on or off.
- **Pull agent logs**  
Selecting the Pull agent logs task collects the activity logs for a specific Symantec DLP Agent in your network.
- **Set log level to info**  
Selecting the Set log level task lets you set the log level of certain logs to Info only. You can also set individual target agent components.
- **Set log level to finest**  
Selecting the Set log level to finest lets you set the log level of certain logs to the finest detail possible. You can also set individual target agent components.

For more information, see the *Symantec Management Platform User's Guide*.

## Creating user tasks

You can create tasks in addition to the predefined tasks on the portal page of the Symantec Management Console. For example, you can create a new task that lets you modify the log level on a non-default logger. The task automatically appears in the task list on the Symantec Management Console portal page. You can delete any tasks that you create from the task list. You cannot delete any predefined tasks.

See [“About Symantec Management Console agent tasks”](#) on page 1101.

### Creating your own tasks

- 1 At the top menu, go to **Manage > Jobs and Tasks**.
- 2 Click the **Create a Task** link.
- 3 Select the task type from the available tree.
- 4 Enter the name of your task.
- 5 Edit the information to create the specifics of the task.
- 6 Set the task server details for which servers you want to associate with this task.
- 7 Click **OK**.

For more on creating your own tasks, see the *Symantec Management Platform User's Guide*.

See [“About the Symantec Management Console”](#) on page 1097.

## About Symantec DLP Agent Installation

You can install the agent software using either automated methods or you can install the agent software manually.

Before you begin, make sure that you have installed and configured an Endpoint Server. If you are using the Symantec Management Console (SMC) to install you agents, the SMC must also be installed before you can begin agent installation.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## What gets installed for Symantec DLP Agents

When the Symantec DLP Agent is installed onto your endpoint computer, a number of components are also installed. These components combine to form the Symantec DLP Agent. Do not disable or modify any of these components or your Symantec DLP Agent may not function correctly.

**Table 68-1** Installed components

Component	Description
Driver (v fsmfd.sys)	Detects any activity in the endpoint file system and relays the information to the Symantec DLP Agent service. This driver is installed at <i>Windows_dir\System32\drivers</i> . For example, <i>c:\windows\System32\drivers</i> . All other agent files are installed into the agent installation directory.
Driver (tdifd105.sys)	Intercepts network traffic (HTTP, FTP, and IM protocols) on the endpoint computer. After the Symantec DLP Agent analyzes the content, the tdifd105.sys driver either allows the information packets to transfer over the network or it blocks them.
Driver (vrtam.sys)	Monitors the process creation and destruction and send notifications to the Symantec DLP Agent. The driver monitors the applications that are configured as part of the Endpoint Application Control; for example, CD/DVD applications.
Symantec DLP Agent service	Receives all information from the driver and relays it to the Endpoint Server. During installation, the Symantec DLP Agent is listed under the task manager as edpa.exe.
Watchdog service	Automatically checks to see if the Symantec DLP Agent is running. If the Symantec DLP Agent has been stopped, the watchdog service restarts the Symantec DLP Agent. This relationship is reciprocal.

The Symantec DLP Agent service creates the following files:

- Two log files (edpa.log and edpa\_ext.log), created in the installation directory.
- Each Symantec DLP Agent maintains an encrypted database at the endpoint. The database stores incident information and the original file that triggered the incident, if needed. Depending on the detection methods used, the Symantec DLP Agent either analyzes the content locally or sends it to the Endpoint Server for analysis.
- Two additional databases are installed to maintain and contain non-matching entries for rules results caching (RRC). See [“About rules results caching \(RRC\)”](#) on page 1065.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About preinstallation steps for Symantec DLP Agents

Before you install the Symantec DLP Agent, identify all security applications that run on your endpoint computers. Then configure those applications to allow the Symantec DLP Agents to function fully. Some applications generate alerts when they detect the installation or initial launch of a Symantec DLP Agent. Such alerts reveal the presence of Symantec DLP Agents and they sometimes let users block the Symantec DLP Agent entirely.

Check the following applications:

- Antivirus software
- Firewall software

Make sure that your antivirus software and firewall software recognize the Symantec DLP Agents as legitimate programs.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## Using the Elevated Command Prompt with Windows Vista and Windows 7

If you install agents on an endpoint computer that runs Windows Vista or Windows 7, you must run the command prompt in **Elevated Command Prompt** mode. This step is required because of the nature of the Windows Vista 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 Vista

- 1 Right-click the command prompt icon in the **Windows Start** menu.
- 2 Select **Run as Administrator**.

The command prompt starts in Elevated Command Prompt mode. You can now install the Symantec DLP Agents on the endpoint computer.

If you install on Windows 7, the procedure for using the Elevated Command Prompt mode follows.

### 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.
- 3 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.
- 5 The command prompt starts in Elevated Command Prompt mode. Install the Symantec DLP Agents on the endpoint computer using this command prompt.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About Symantec DLP Agent security

Symantec Data Loss Prevention uses Advanced Encryption Standard (AES) technology to secure communications between the Endpoint Server and the Symantec DLP Agent. Symantec Data Loss Prevention also uses AES to secure the Symantec DLP Agent database file.

AES is a symmetric-key encryption technology that supports key sizes of 128, 192, and 256 bits.

Symantec Data Loss Prevention uses the following sets of AES keys:

- One to secure the agent database file
- One to authenticate the Endpoint Server to the Symantec DLP Agent
- One to encrypt traffic between the Endpoint Server and Symantec DLP Agent

The database file key is only used at the Symantec DLP Agent. However, the authentication key and the traffic encryption keys must be shared between the Endpoint Server and Symantec DLP Agent. By default, Symantec Data Loss

Prevention uses the predefined 128-bit database and authentication keys. The traffic encryption key is a randomly generated session key that is negotiated every time the Symantec DLP Agent connects to the Endpoint Server.

Although the information in Symantec Data Loss Prevention is secure, you should change the default keys. You can change the database key, the authentication key, and the AES key size (128, 192, 256). You should change these default settings (either change them to use unique keys or change the key size) before you deploy the Symantec DLP Agents. Symantec Data Loss Prevention includes the `endpointkeytool` utility to generate the authentication key. The `endpointkeytool` utility also lets you create a tools-password that you need to access the other endpoint tools.

See [“About Endpoint tools”](#) on page 1135.

See [“About endpointkeytool utility”](#) on page 1136.

See [“Running the endpointkeytool utility”](#) on page 1137.

A new traffic encryption key is randomly generated each time a Symantec DLP Agent connects to the Endpoint Server. The key is discarded as soon as the connection session between server and agent ends. The traffic encryption key is always unique for each Symantec DLP Agent connection session. The authentication key is shared in common by the Endpoint Server with all Symantec DLP Agents.

By default, Symantec Data Loss Prevention is configured to use the 128-bit key size to protect communication between the Endpoint Server and Symantec DLP Agents. However, the bit size of the authentication key can be increased to enhance encryption. If the bit size for the authentication key is increased, the bit size of the traffic encryption key is automatically increased. In this way, the two encryption keys always have matching bit-sizes. The bit size of the authentication key can only be changed before you install Symantec DLP Agents.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About the authentication key

All Symantec Data Loss Prevention customers are provided with a default 128-bit authentication key that is hard-coded into the product. This authentication key works well for many customers, but you have the option to generate a new authentication key. Several factors need to be considered before you replace an authentication key.

The benefits of generating a new authentication key are as follows:

- A new AES key isolates you from other Symantec customers that use the default key. The default configuration is to use the authentication key that is hard-coded into Symantec Data Loss Prevention. All Symantec Data Loss Prevention customers use the same authentication key unless the key is changed.
- The encryption security for data traffic can be enhanced by increasing the size of the authentication key to 192- or 256-bit. The greater bit size makes compromising data security even more difficult.

The drawbacks to generating a new authentication key are as follows:

- Advance planning is required before the Symantec DLP Agents are installed. You cannot change the authentication key after the Agents are installed.
- The United States government regulates the use of 192-bit and 256-bit AES keys. Export laws highly restrict the use of these keys outside of the United States. System performance may also suffer by using larger key sizes.

You can change the authentication key with the `endpointkeytool` utility.

See [“About endpointkeytool utility”](#) on page 1136.

See [“Running the endpointkeytool utility”](#) on page 1137.

See [“About Endpoint tools”](#) on page 1135.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About the watchdog service

The watchdog service is deployed with the Symantec DLP Agent. The watchdog is a service that ensures that the Symantec DLP Agent is running and active. This relationship is reciprocal. If the Symantec DLP Agent does not receive regular requests from the watchdog service, it automatically restarts the watchdog service. This reciprocal relationship ensures that the Symantec DLP Agent is always running and active.

For added security, the watchdog service is given a non-obvious name. In the **Task Manager** list, the watchdog service is named `wdp.exe`. The watchdog service contains a non-obvious name so users are not able to easily find the service and try to stop it.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About Endpoint Server redundancy

You can configure the Symantec DLP Agent to connect to multiple Endpoint Servers. Multiple Endpoint Servers enable incidents and events to be sent to the Enforce Server in a timely way if an Endpoint Server becomes unavailable. For example, assume that an Endpoint Server becomes unavailable because of a network partition. The Symantec DLP Agent, after a specified amount of time, connects to another Endpoint Server to transmit the incidents and events that it has stored. The Symantec DLP Agent makes a best effort to fail over to a different Endpoint Server only when the current Endpoint Server is unavailable. If the original Endpoint Server is unavailable, the Agent attempts to connect to another Endpoint Server in the configured list. By default, the Symantec DLP Agent tries to reconnect to the original Endpoint Server for 60 minutes before it connects to another Endpoint Server.

When a Symantec DLP Agent connects to a new Endpoint Server, it downloads the policies from that Endpoint Server. It then immediately begins to apply the new policies. To ensure consistent incident detection after a failover, maintain the same policies on all Endpoint Servers to which the Symantec DLP Agent may connect.

For Endpoint Discover monitoring, if a failover occurs during a scan, the old Endpoint Discover scan is aborted. The Symantec DLP Agent downloads the new Endpoint Discover policy from the new Endpoint Server and immediately runs a new scan.

You must specify the list of Endpoint Servers when you install the Symantec DLP Agents. The procedure for adding a list of Endpoint Servers appears under each method of installation. You can specify either IP addresses or host names with the associated port numbers. If you specify a host name, the Symantec DLP Agent performs a DNS lookup to get a set of IP addresses. It then connects to each IP address. Using host names and DNS lookup lets you make dynamic configuration changes instead of relying on a static install-time list of stated IP addresses.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## About the AgentInstall.msi package

Symantec DLP Agents are installed, configured, or upgraded on endpoint computers using the AgentInstall.msi package (or AgentInstall64.msi package for Windows 7 64-bit platforms). The Symantec Management Console or Systems Management Server (SMS) executes the package in Silent Mode using the Windows `msiexec` installer. You can also run the package installer interactively on an endpoint computer by executing the AgentInstall.msi package itself.

The AgentInstall.msi package accepts various configuration properties regardless of which method you choose to install the Symantec DLP Agents. [Table 68-2](#) describes the required properties and optional properties for AgentInstall.msi and AgentInstall64.msi.

**Table 68-2** AgentInstall.msi and AgentInstall64.msi Properties

Property Name	Description	Required or Optional	Default Value
ENDPOINTSERVER	Specifies the host name or IP address of one or more Endpoint Servers that are separated by semicolons. An optional port number can follow each host name or IP address. If no port number is specified, the default port number is used. The default number is 8000.  For example: <code>ENDPOINTSERVER="epserver.company.com; 10.67.20.36:8002"</code>	Required	None
SMC	This property is deprecated. The installer ignores any value that you specify for SMC.	Deprecated	None
ENABLEFIPS	Enables FIPS-compliant encryption. Set this property to "Yes" to enable FIPS encryption if needed.  See <a href="#">"Installing the Symantec DLP Agent on FIPS-compliant computers"</a> on page 1116.	Optional	No
ENABLEWATCHDOG	Enables the watchdog service. Specify "No" to disable the service.	Optional	Yes

**Table 68-2** AgentInstall.msi and AgentInstall64.msi Properties (*continued*)

Property Name	Description	Required or Optional	Default Value
KEY	The authentication key that the Symantec DLP Agent and Endpoint Server use to establish a secure connection. Agents include a default authentication key, but you can create your own key using the <code>endpointkeytool</code> utility. To use your own key, specify it with the <code>KEY</code> parameter during deployment and installation. If you decide to specify the key after installing Symantec DLP Agents, you must reinstall the Symantec DLP Agents to specify the key.  See " <a href="#">About endpointkeytool utility</a> " on page 1136.	Optional	None (A common default key is used.)
HIDESMCICON	Displays or hides the Symantec Management Console icon. Use this parameter only if you have the Symantec Management Console installed and you do not want general users to see the icon.	Optional	No
SERVICENAME	Specifies the Symantec DLP Agent service name that appears in the service list of the endpoint computer. The Symantec DLP Agent appears as <code>edpa.exe</code> on the computer's task list.	Optional	EDPA
STARTSERVICE	Determines whether the Symantec DLP Agent and watchdog service are started on the endpoint computer after installation. Set this property to No to disable starting the services after installation.	Optional	Yes
WATCHDOGNAME	Specifies the watchdog service name that appears in the service list on the endpoint computer. The watchdog appears as <code>wdp.exe</code> in the Task Manager.	Optional	WDP

The `msiexec` installer also has several public properties that are commonly used when you install the `AgentInstall.msi` package. These properties include:

■ **ARPSYSTEMCOMPONENT**

This property can prevent the Symantec DLP Agent from appearing in the endpoint computer's Add or Remove Programs (ARP) list. If you set this property to 1, the Symantec DLP Agent does not appear in the list. By default, the property is set to 0, which allows the Symantec DLP Agents to appear in the ARP list.

■ **INSTALLDIR**

This property specifies the installation directory. The default installation directory is `install_dir\Manufacturer\Endpoint Agent`. For example, `c:\Program Files\Manufacturer\Endpoint Agent`.

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## Installing Symantec DLP Agents with the Symantec Management Console

You can use Symantec Management Console to install Symantec DLP Agents. The Symantec Management Console installs Symantec DLP Agent components semi-automatically onto your endpoint computers.

If you previously purchased and installed Symantec Management Console, you can use the Symantec Management Console software to install Symantec DLP Agents. The Symantec Management Console installs Symantec DLP Agent components semi-automatically onto your endpoint computers. Note that Symantec Data Loss Prevention does not include Symantec Management Console.

---

**Note:** To install the Symantec DLP Agents with the Symantec Management Console, you must have previously used the Computer Discovery feature of the Symantec Management Console. You must first install the Symantec Management Agent.

See [“About Symantec Management Console reporting”](#) on page 1100.

---

The Symantec Management Console uses a system of packages, programs, and advertisements to install the Symantec DLP Agent. Packages contain the reference information to the installation directory. Programs are the installation files themselves and contain the installation parameters. You must specify the Endpoint Server(s) that you associated with the Symantec DLP Agent in the command line in the installation program. Advertisements let you specify on which endpoint

computers you want to install the Symantec DLP Agent and when you want that installation to occur.

You must always install the AgentInstall.msi or AgentINStall64.msi package from a local directory. If you do not install from a local directory, some functions of the Symantec DLP Agent are disabled.

---

**Note:** Symantec Data Loss Prevention supports both 32-bit and 64-bit operating systems. Symantec DLP Agent links that are marked with **(x86)** install or modify Symantec DLP Agents for 32-bit systems. Symantec DLP Agent links that are marked with **(x64)** install or modify Symantec DLP Agents for 64-bit systems.

---

#### To install the Symantec DLP Agent with the Symantec Management Console

- 1 On the DLP Portal page, click the **Install Symantec DLP agent (*bit information*)** link where (*bit information*) is the operating system you want.
- 2 In the right-hand pane, click the drop-down menu next to the red **Off** icon and select the green **On** icon.
- 3 Make sure that the Program name field is set to **Install DLP Agent**.
- 4 Under the **Applied to** section, select the **Apply to > Computers** menu option. Add filter rules as necessary to select a subset of endpoint computers.  
The Symantec DLP Agent is installed only on the computers listed.
- 5 Click **OK**.
- 6 If you want to schedule the installation for a later time, specify those settings in the **Schedule** section.
- 7 Click **Save changes**.

After you have saved the changes for the installation, view the status of the installation on the DLP Portal page.

## Installing Symantec DLP Agents with an unattended installation

You can use an unattended installation process by using a systems management software product (SMS) to install Symantec DLP Agents to endpoint computers. You must always install the AgentInstall.msi package from a local directory. If you do not install from a local directory, some functions of the Symantec DLP Agent are disabled.

### To perform an unattended installation

- 1 In your systems management software package, specify the AgentInstall.msi or AgentInstall64.msi package.
- 2 Specify the AgentInstall.msi installation properties.  
See [“About the AgentInstall.msi package”](#) on page 1108.
- 3 Specify the `msiexec` properties.  
Optional properties for the `msiexec` utility.  
See [“About the AgentInstall.msi package”](#) on page 1108.
- 4 Specify any optional properties for the `msiexec` utility.  
See [“About the AgentInstall.msi package”](#) on page 1108.

For details on entering this information into your particular systems management software, see the software product documentation.

When you install the Symantec DLP Agent, your systems management software issues a command to the specified endpoints. The following is an example of what the command might look like:

```
msiexec /i AgentInstall.msi /q TARGETDIR="C:\Program  
Files\Manufacturer\Symantec DLP Agent\" ARPSYSTEMCOMPONENT="1"  
  
ENDPOINTSERVER="epserver:8001" SMC="smcserver"  
  
SERVICENAME="ENDPOINT" WATCHDOGNAME="WATCHDOG"
```

In this command:

`msiexec` is the Windows command for executing MSI packages.

`/i` specifies the name of the package.

`/q` specifies a silent install.

`TARGETDIR` and `ARPSYSTEMCOMPONENT` are optional properties to `msiexec`.

`ENDPOINTSERVER`, `SMC`, `SERVICENAME`, and `WATCHDOGNAME` are properties for the AgentInstall.msi package.

Symantec Data Loss Prevention includes an example installation command in `install_dir\Endpoint\install_agent.bat`.

After you install the agents, the Symantec DLP Agent service automatically starts on each endpoint computer. Log on to the Enforce Server and go to **System > Agents > Overview**. Verify that the newly upgraded agents are registered (that the services appear in the list).

---

**Note:** Do not rename the Agentinstall.msi file for any reason. If you rename this file, your systems management software cannot recognize the file and the installation fails.

---

---

**Note:** Some aspects of the Symantec DLP Agent installation may require you to restart the endpoint computer.

---

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## Installing Symantec DLP Agents manually

You can install Symantec DLP Agents manually on your endpoints by using the AgentInstall.msi or AgentInstall64.msi (for Windows 7 64-bit platforms) package.

### To install Symantec DLP Agent manually

- 1 Log on to the endpoint computer as an administrator.
- 2 Copy the AgentInstall.msi or AgentInstall64.msi file to the endpoint computer and double-click the file.

The Symantec DLP Agent installation wizard starts up, displaying the Symantec DLP Agent setup panel.

- 3 Click **Next** to accept the copyright agreement.
- 4 Click **Next** to accept the license agreement.

---

**Note:** If your computer is not already running Windows Installer 3.1, the Symantec DLP Agent installer initiates the installation of that program. In this case, you are prompted to restart the computer after the Windows Installer installation. Upon restart, the Symantec DLP Agent installer resumes.

---

- 5 Type the appropriate values in the following fields:
  - **Endpoint Servers (required)**  
Enter the hostname or IP address of at least one Endpoint Server. For example, server.company.com. This value must be consistent with the **Agent Listener > Bind Address (Host/IP)** value you set for the Endpoint Server on the **Symantec Data Loss Prevention Enforce Server > Configure Server page**. If you use a non-default port number, specify it after the server name. For example, server.company.com:8001.

---

**Note:** You can specify more than four Endpoint Servers. To do so, use any of the four available text fields to enter a list of hostnames or IP addresses separated by semicolons. For example, “epserver1.company.com; epserver2.company.com; epserver3.company.com; epserver4.company.com; 10.67.20.36:8002.”

---

- **Encryption Key (optional)**  
You may enter a custom authentication key that the Symantec DLP Agents and Endpoint Server use to establish a secure connection. Agents include a default authentication key, but you can also create your own key using the `endpointkeytool` utility. To use your own key, specify it with the `KEY` parameter during deployment and installation. If you decide to use a custom key after installing Symantec DLP Agents, you must reinstall the Symantec DLP Agents to specify the key.
- **DLP Agent Service Name (optional)**  
You may edit the Symantec DLP Agent service name that appears in the service list of the endpoint computer.
- **DLP Watchdog Service Name (optional)**  
You may edit the watchdog service name that appears in the service list of the endpoint computer.

**6** Click **Next**.

**7** Accept the default installation directory or enter a new one, and then click **Next**.

The default is `c:\Program Files\Manufacturer\Endpoint Agent`.

**8** On the Confirm Installation screen that appears, click **Install**.

The installation takes a few moments. When it finishes, the Installation Complete screen appears.

**9** Click **Finish**.

**10** Go to **Start > Control Panel > Administrative Tools**, and then double-click **Services**. Find the Symantec DLP Agent service (listed under the name you typed in the Service Name field during installation). Make sure that it is running.

The Symantec DLP Agent now monitors the endpoint.

**11** Log on to the Enforce Server and go to **System > Agents > Overview**.

**12** Verify that the Symantec DLP Agent is registered (appears in the list).

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

## Installing the Symantec DLP Agent on FIPS-compliant computers

The Federal Information Processing Standards 140-2 (FIPS) are federally defined standards on the use of cryptography. Using the FIPS encryption option is not generally recommended for most customers because it requires additional computational overhead. Before you install FIPS, you must contact your Symantec representative. You should use the FIPS encryption option only if your organization must comply with FIPS regulations (typical organizations include US government agencies and departments). If you do not select the FIPS encryption option, the installer defaults to the standard encryption option. You cannot switch to a different option except by reinstalling Symantec Data Loss Prevention. When a re-installation is required, old incidents are not preserved. All of your Symantec Data Loss Prevention servers and agents must run either one or the other encryption option; you cannot mix encryption options. If your organization uses Internet Explorer to access the Enforce Server, then you also need to ensure that Internet Explorer is configured to use FIPS.

Contact Symantec Data Loss Prevention support for more information.

### To include the FIPS-compliant MSI parameter

- ◆ Include the following parameter in your MSI package:

```
msiexec /i AgentInstall.msi ENABLEFIPS="Yes"
```

See [“How to implement Endpoint Discover”](#) on page 1067.

See [“How to implement Endpoint Prevent”](#) on page 1075.

# Managing Symantec DLP Agents

This chapter includes the following topics:

- [About Symantec DLP Agent administration](#)

## About Symantec DLP Agent administration

You install and manage the Symantec DLP Agents through the Symantec Management Console. After you install the Symantec DLP Agents, you can administer them from the Enforce Server. The Enforce Server lets you view events for the Symantec DLP Agents, agent information, and generate reports for the agent events.

The Enforce Server contains an overview of the Symantec DLP Agents, a log of the Symantec DLP Agent events, and an upgrade utility. The following explains the overview and the event log pages.

To access the agent pages, open **Enforce Server > System > Agents**.

See [“Using the agents overview screen”](#) on page 1117.

See [“Agent management events screen”](#) on page 1124.

## Using the agents overview screen

You can see the status of each Symantec DLP Agent on the agent overview screen. The statuses are described by individual icons displayed next to each agent. You can also perform agent tasks on any selected agents. Use the checkboxes to select the agents that you want to modify.

Use the Action button to perform on of the following actions:

- Change Endpoint Server
- Delete
- Disable
- Enable
- Pull Logs
- Remove Under Investigation
- Restart
- Set Under Investigation
- Shut Down

See “[Agent overview actions](#)” on page 1122.

Agent 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 agents by the endpoint computer name.

**Table 69-1** Agent overview screen

Section	Description
Status	

**Table 69-1** Agent overview screen (*continued*)

Section	Description
	<p>Current status of the agent.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> <li>■ <b>Healthy</b> Indicates the agent service and file-system driver are running, that the cache is created and available, and that the connection functions as expected.</li> <li>■ <b>Warning</b> Indicates the agent may need attention. For example, Symantec Data Loss Prevention assigns this status when the endpoint data share nears its storage limit.</li> <li>■ <b>Down</b> Indicates the agent is down and needs immediate attention. For example, Symantec Data Loss Prevention assigns this status when the data share is full or unavailable, or when the connection is lost.</li> <li>■ <b>Shut Down</b> Indicates that the agent has been shut down either through the Shut Down agent task or when the endpoint computer was shut down.</li> <li>■ <b>Disabled</b> Indicates that the agent has been disabled through the Disable agent task.</li> <li>■ <b>Under Investigation</b> 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. You can set the Under Investigation status with any other agent status.</li> <li>■ <b>Troubleshooting</b> Indicates that a troubleshooting task is either running on the agent or that a</li> </ul>

**Table 69-1** Agent overview screen (*continued*)

Section	Description
	<p>troubleshooting task has just expired on an agent.</p> <p>You can set the Troubleshooting status with any other agent status.</p>
Machine Name	The endpoint computer name.
Recent error messages	<p>Symantec Data Loss Prevention displays one or more messages that are related to any events that change agent status to Down status. Each message shows the time and summary of the event that triggered the status change. To see a list of events for a particular agent, click on the relevant agent entry in the <b>Agent Management Overview</b> list.</p>
Endpoint Server	The Endpoint Server to which the agent is registered.
IP	The endpoint computer IP address.
Version	Agent version number.
Connection	Current agent connection status.
Last Connection Time	The date and time that the specific Symantec DLP Agent last connected to the Endpoint Server.

You can summarize the agent overview page 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 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.

See [“About filters and summary options for reports”](#) on page 761.

See [“Agent management events screen”](#) on page 1124.

## Agent overview actions

The following table describes the available agent overview actions that you can take on any Symantec DLP Agent.

See [“Using the agents overview screen”](#) on page 1117.

**Table 69-2** Agent overview actions

Action	Description
Change Endpoint Server	<p>Lets you change the Endpoint Server to which the agent connects.</p> <p>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.</p>
Delete	<p>Deletes the agent</p> <p>When you delete an agent, you remove that agent and all associated events from the Endpoint Server. It is no longer visible to or connected to the Endpoint Server. Deleting an agent from the Endpoint Server does not mean that it has been uninstalled from the endpoint computer.</p>
Disable	<p>Disables the agent</p> <p>Disabling the agent does not delete the agent from the Endpoint Server. Disabling an agent disables all monitoring on that endpoint computer. The associated events are still visible on the Endpoint Server. Unlike deleted agents, disabled agents can be re-enabled.</p>
Enable	<p>Enables disabled agents</p> <p>Enabled agents automatically reconnect with the Endpoint Server and obtain the most current policies. Enabling an agent enables monitoring on that endpoint computer. Enabled agents can log events on the Endpoint Server.</p> <p><b>Note:</b> Any updates to the associated policies are not sent to the agent until the agent is enabled and restarted.</p>

**Table 69-2** Agent overview actions (*continued*)

Action	Description
Pull Logs	<p>Let's 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.</p> <p>Pulling agent logs is a two-step process:</p> <ul style="list-style-type: none"> <li>■ Pull the agent logs from the endpoint computer to the Endpoint Server</li> <li>■ Collect the agent logs from the Endpoint Server through the Enforce Server</li> </ul> <p>When the logs are pulled from the endpoint computer, 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 computer at a time.</p> <p>Access the logs from the Enforce Server Logs page. Go to: <b>System &gt; Servers &gt; Logs &gt; Collection</b>.</p> <p>See <a href="#">“Collecting server logs and configuration files”</a> on page 236.</p>
Remove Under Investigation	Removes the Under Investigation designation from the selected agents.
Restart	Restarts the specified agent
Set Under Investigation	<p>Sets an Under Investigation status on the specified agent.</p> <p>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.</p>

**Table 69-2** Agent overview actions (*continued*)

Action	Description
Shut Down	Shuts down the specified agent.  After the agent has been shut down, you cannot restart it through the Enforce administration console. Agents can only be restarted through the Symantec Management Console (SMC) or on the individual endpoint computer.

You can view the most current information regarding the agent actions in a Knowledge Base article. Logon to the Altiris Knowledge base at: <https://kb1vontu.altiris.com> and search for the article *About Symantec DLP Agent troubleshooting tasks*. Alternately, after you logon, you can search for the article number 54083.

## Agent management events screen

The Agent Management Events screen lists the events that have occurred on agents. Such events 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 69-3** Agent Management Event screen

Entry	Description
Checkboxes	Checkboxes let you select which events to delete. You can select one or more events to delete. 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 <b>all</b> incidents in the report.)

**Table 69-3** Agent Management Event screen (*continued*)

Entry	Description
Type	The event type, which includes the following possible values: Severe Agent Information OK
Time	Event date and time.
Endpoint Server	The name of the Endpoint Server that is associated with the event.
Machine Name	Endpoint computer IP address or host name.
Category	Event category, such as Agent Service Status, Connection Status, File-System Driver, or data store.
Sub-Category	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.

You can summarize the agent overview page 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 events 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.

See [“About filters and summary options for reports”](#) on page 761.

### About agent events filter options

In addition to the default Date filter, you can filter on event type (severe, warning, informational, or under investigation), the Endpoint Server that is associated with the agent, the event summary information, and the endpoint computer name.

You can also filter on the categories and sub-categories of information that Symantec Data Loss Prevention uses to assess general agent status.

**Table 69-4** Agent event filter options

Filter	Description
Category	The category to which the event belongs. The type or category of event assists to designate the severity of the event. For example, a software upgrade event is of a lower severity than a software compatibility event. Searches can include or exclude categories of events.
Machine Name	The endpoint machine on which the agent is running. Searches can include, exclude, or search based on exact matches. If only one machine used, then excluding that machine results in no matches.
Server	The server to which the agent events belong. You can include or exclude all events for a single server.
Sub Category	The subcategory for event categories. Each category is separated by different subcategories. For example, the Configuration Update category contains the subcategories Config Error and Config Success.
Summary	The essential information about each event. You can filter on keywords or sentence strings. Filters can include, exclude, or search on exact matches for summary descriptions.
Type	The type of event listed. You can list events as Severe, Warning, or Info.

After you select a filter option, you must select the sub-category for the filter. For example, if you choose to filter on Category, you must then choose a specific category, such as Connection Status.

See [“Agent management events screen”](#) on page 1124.

## About Symantec DLP Agent removal

You may need to uninstall the Symantec DLP Agent from your endpoint computers. You can uninstall Symantec DLP Agents in the following ways:

**Table 69-5** Removing the Symantec DLP Agent

[Removing Symantec DLP Agents with Symantec Management Console](#)

[Removing Symantec DLP Agents manually](#)

[Removing Symantec DLP Agents with System Management Software](#)

## Removing Symantec DLP Agents with Symantec Management Console

You can remove the Symantec DLP Agent and the Symantec Management Agent from your endpoint computers using the Symantec Management Console.

---

**Note:** Symantec Data Loss Prevention supports both 32-bit and 64-bit operating systems. Symantec DLP Agent links that are marked with **(x86)** install or modify Symantec DLP Agents for 32-bit systems. Symantec DLP Agent links that are marked with **(x64)** install or modify Symantec DLP Agents for 64-bit systems.

---

### To uninstall the Symantec DLP Agent with Symantec Management Console

- 1 From the left-hand navigation window, go to: **Data Loss Prevention Portal > Configuration > V11.0 Agent Deployment (*bit information*) > Uninstall DLP Agent (*bit information*)** where (*bit information*) is either the 32-bit or 64-bit system folder.
- 2 On the top-right portion of the page, click the red **Off** icon and select the green **On** icon from the drop-down menu.
- 3 Make sure that the **Program name** field is set to **Uninstall Symantec DLP Agent**.
- 4 Under the **Applied to** section, click the **Apply to** option and select **Computers**. Add filter rules as necessary to select a subset of endpoint computers.  
 The Symantec DLP Agent is uninstalled only from the computers listed.
- 5 Click **Save changes**.

---

**Note:** You can also schedule the uninstallation for a later time. Use the Task Scheduler to schedule the time you want to uninstall the agents.

---

For more information on uninstallation options using the Symantec Management Console, see the *Symantec Management Platform User's Guide*.

See "[About Symantec DLP Agent removal](#)" on page 1126.

See [“About the Symantec Management Console”](#) on page 1097.

## Removing Symantec DLP Agents with 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.

- 3 Click **OK**.

The Symantec DLP Agent uninstalls.

### To remove the agent manually if the agent does not appear in the ARP

- 1 Open the command prompt window.
- 2 Enter the following command where `{guid}` is the product code. You can add several other options to this command prompt:

```
msiexec /x {guid}
```

**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:

```
/QN: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 1126.

### Removing agents with Windows 7 or Vista

If you uninstall the agents from an endpoint computer that runs Windows Vista or Windows 7, you must run the command prompt in **Elevated Command Prompt** mode. This step is required because of the nature of the Windows Vista 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 Vista

- 1** Right-click the command prompt icon in the **Windows Start** menu.
- 2** Select **Run as Administrator**.

The command prompt starts in Elevated Command Prompt mode. You can now install the Symantec DLP Agents on the endpoint computer.

If you are installing on Windows 7, the procedure for using the Elevated Command Prompt mode follows.

### 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.
- 3 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.
- 5 The command prompt starts in Elevated Command Prompt mode. Install the Symantec DLP Agents on the endpoint computer using this command prompt.

See [“About Symantec DLP Agent removal”](#) on page 1126.

### Removing Symantec DLP Agents manually

You can uninstall Symantec DLP Agents manually. Manual uninstallation is only possible if you configured the Symantec DLP Agent to appear in the endpoint computer **Add or Remove Programs** list during deployment.

See [“About Symantec DLP Agent Installation”](#) on page 1102.

#### To uninstall the agent manually

- 1 Go to **Start > Control Panel** and double-click **Add or Remove Programs**.
- 2 Select **Agent Install**.
- 3 Click **Remove**.  
If you use Windows Vista, you are prompted to use the Elevated Command Prompt mode.

See [“About Symantec DLP Agent removal”](#) on page 1126.

# About application monitoring

This chapter includes the following topics:

- [About application monitoring](#)
- [Adding an application](#)

## About application monitoring

Application monitoring lets you monitor third-party applications for IM, email, or HTTP/S clients. By default, Symantec Data Loss Prevention only monitors first-party applications such as AIM, Microsoft Outlook, or Mozilla Firefox. Examples of third-party applications include Skype, Mozilla Thunderbird, or Google Chrome. Any application that is not specifically monitored by Symantec Data Loss Prevention must be added to the Application Monitoring page before Symantec Data Loss Prevention can begin monitoring. For example, if your company uses Mozilla Thunderbird, you must add Mozilla Thunderbird to the Application Monitoring page. You need to add the application because Mozilla Thunderbird is not monitored by default. After Mozilla Thunderbird is added, Symantec Data Loss Prevention monitors the file attachments that are sent by the email client through the network.

Additionally, you can configure global changes to default applications. 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 fingerprinting page. The applications on this page are only the

applications that you want to modify for network, print/fax, Clipboard, or file system monitoring.

The Application Monitoring page displays the list of currently monitored CD/DVD applications. If you do not see the specific CD/DVD application you need, you must add that application to the list.

---

**Note:** You can remove any application that you add, but you cannot remove a pre-populated application.

---

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.

See [“Adding an application”](#) on page 1132.

---

**Note:** Small files of less than 64 bytes are not detected when read by a third-party application. Files over 64 bytes in size are detected normally.

---

## Adding an application

The Add Application Monitoring page can be used to add third-party applications to monitoring policies. Third-party applications can include the following types of applications:

- CD/DVD applications (for example, Roxio)
- Internet browsers (for example, Google Chrome)
- IM applications (for example, Skype)
- SMTP applications (for example, Mozilla Thunderbird)

### Adding an application

- 1 Under the Application Information section, You must enter at least one of the following fields:
  - Name
  - Binary Name
  - Internal Name
  - Original Filename

- **Publisher Name**

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.

- 2 Under the Application Monitoring Configuration section, select one or more of the following monitoring options:

- Network Access
- Print/Fax
- Send to Clipboard
- Filesystem Activity

- 3 If you have selected Filesystem Activity, you can select one of the following options:

- Monitor Application File Access
- Monitor writing to CD/DVD

Selecting the Application File Access or CD/DVD options lets you choose to monitor the files that the application opens or the files that the application reads.

See “[About application monitoring](#)” on page 1131.



# Using Endpoint Server 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. These tools are contained within the `VontuAgentInstaller.zip` file. Install these tools into 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 work properly. Each tool requires a password to operate. A generic tools password is generated during your installation.

You can change the password using the `endpointkeytool` and create a tools-specific password. Symantec recommends that you install the tools into the Symantec DLP Agent installation directory that contains the keystore files. The `endpointkeytool` utility, however, is installed on Enforce and can be found at `Vontu\Enforce\Protect\bin`.

See “[About endpointkeytool utility](#)” on page 1136.

The following is a list of the available Endpoint tools:

[About endpointkeytool utility](#)

[Shutting down the agent and the watchdog services](#)

[Inspecting the database files accessed by the agent](#)

[Viewing extended log files](#)

You can also perform some of these tasks with the Symantec Management Console.

See [“About Symantec Management Console agent tasks”](#) on page 1101.

## Using Endpoint tools with Windows 7 or Vista

If you use Endpoint tools on a computer that runs Windows 7 or Vista, you must run the command prompt in the Elevated Command Prompt mode. This procedure is required because of the nature of the Windows 7 and the Vista operating system. You cannot run the Endpoint tools without using the Elevated Command Prompt mode.

### To initiate the Elevated Command Prompt mode in Windows 7

- 1 From the Windows Start menu, click the **Search programs and files** field. Enter `command`.
- 2 Right-click the command prompt window while simultaneously pressing the **Shift** key.
- 3 Select the **Run as administrator** option.

### To initiate the Elevated Command Prompt mode in Windows Vista

- 1 From the Windows Start menu, right-click the **Command Prompt** icon.
- 2 Select **Run as Administrator**.

The command prompt starts in the Elevated Command Prompt mode. You can now use the Endpoint tools.

See [“About Endpoint tools”](#) on page 1135.

## About endpointkeytool utility

Use the endpointkeytool command-line utility to generate an authentication key and define a tools password. Symantec Data Loss Prevention uses default keys. You must generate your own unique keys to ensure that you do not use the same key as another customer. Back up and secure the files that the endpointkeytool generates. Before you start, make sure that the Endpoint Server is installed but that no Symantec DLP Agents are installed.

---

**Note:** Please check your operating system licensing limitations as some key sizes are not recognized outside of the United States.

---

See [“About Endpoint tools”](#) on page 1135.

See [“Running the endpointkeytool utility”](#) on page 1137.

See [“About Symantec DLP Agent security”](#) on page 1105.

## Running the endpointkeytool utility

The endpointkeytool utility must run under the Symantec Data Loss Prevention operating system user account. By default the account is “protect.” The command options for the endpointkeytool utility are:

Option	Description
<code>-keysize=&lt;128/192/256&gt;</code>	Specifies the bit-size of the generated key file.
<code>-pwd=tools_password</code>	Specifies the password to access the endpoint tools. By default, the password is <i>VontuStop</i> . You must specify a password.
<code>[-dir=directory]</code>	The optional <code>-dir</code> argument specifies the directory where the keystore files are placed.

Unless you specified a different directory with the `-dir` argument, the keystore file `*.endpointRecoveryStore` is created in the `\bin` directory where the endpointkeytool utility resides. By default, the `\bin` directory is `...Enforce\Protect\bin`. This keystore file must be moved to the keystore directory to function.

---

**Note:** If more than one keystore file is in the keystore directory, the Endpoint Server does not start.

---

### To generate an endpointkeytool file

- 1 Under the Symantec Data Loss Prevention user account, run the `endpointkeytool` utility with the needed parameters, for example:

```
endpointkeytool generate -keysize=128 -pwd=VontuStop
```

- 2 Enter a tools password using the parameters `-pwd=tools_password` and `-keysize=128/192/256`. In the command, `tools_password` is the password you want to use and `128/192/256` is the size of the key you want to use.
- 3 Unless you used the `-dir` option to specify where the keystore file is generated, place the keystore file in a safe, memorable directory. Verify that the keystore directory contains only one keystore file.

- 4 Store a copy of the keystore file in a safe location. If anything happens to the keystore file on a Symantec DLP Agent, a copy of the keystore file is available to replace the damaged file.

The Endpoint Server must use the key that is generated at the same `endpointkeytool` session. Any Symantec DLP Agent that uses a different key cannot be authenticated and cannot communicate with the server. An Authentication Failure Endpoint system event is generated if a problem with the keystore file occurs. The Symantec DLP Agent status is shown in the Agent Overview screen of the management console.

- 5 Copy the authentication key into the `KEY` parameter for the MSI installation script for installing Symantec DLP Agents. This procedure ensures that the installation script installs all Symantec DLP Agents with the same authentication key. If the `KEY` parameter is left empty, then the Symantec DLP Agents use the default key.

The Endpoint Server has a keystore directory that is located at `Vontu/Protect/keystore`. An empty keystore directory indicates that Symantec Data Loss Prevention is using the default embedded keystore file. After the generated keystore file is copied into the keystore directory, it overrides the default keystore file.

If you forget your tools password, you can recover it using the `endpointkeytool recover` option:

```
endpointkeytool recover [-dir=output_dir]
```

- 6 Restart the Endpoint Server through the Enforce console.

See [“About Endpoint tools”](#) on page 1135.

See [“About Symantec DLP Agent security”](#) on page 1105.

See [“About endpointkeytool utility”](#) on page 1136.

See [“About the authentication key”](#) on page 1106.

## 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 1135.

## Inspecting the database files accessed by the agent

The vontu\_sqlite3.exe tool enables you to inspect the database files that are used by the Symantec DLP Agent. 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.

### To run the vontu\_sqlite3.exe tool

- 1 From the Symantec DLP Agent installation directory, run:

```
vontu_sqlite3 -db=database_file [-p=password]
```

where *database\_file* is your database file and *password* is your specified tools password.

All Symantec Data Loss Prevention database files are present in the Symantec DLP Agent installation directory and end in the \*.ead extension. After you run the command, you are prompted for your password.

- 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 1135.

## Viewing extended log files

The `logdump.exe` tool lets you view the extended log files for Symantec DLP 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 DLP Agent log files.

### To run the log dump tool

- ◆ From the Symantec DLP Agent installation directory, run:

```
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 DLP 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.

From this view, you can print the contents of another log.

### To print the contents of another log

- 1 From the command window, run:

```
logdump -log=log_file -p=password > deobfuscated_log_file_name
```

- 2 Enter the password again to print the log.

See [“About Endpoint tools”](#) on page 1135.

## 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 492.

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 1141.

**Table 71-1** Device ID utility example output

Result	Description
Volume	The volume or mount point that the <code>DeviceID.exe</code> 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
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 1140.

See [“About endpoint device detection”](#) on page 492.

### To use the Device ID utility

- 1 Obtain the `DeviceID.exe` utility.

This utility is available with the Endpoint Sever utilities package.

See [“About Endpoint tools”](#) on page 1135.

- 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.

**4** 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 71-1](#) on page 1141.

**6** Use the `DeviceID` utility to evaluate the proposed regex string against a device that's currently connected.

See [Table 71-2](#) on page 1142.

**7** Use the regular expression patterns to configure endpoint devices for detection.

See [“Creating and modifying endpoint device configurations”](#) on page 497.

**Table 71-2** Device ID regex evaluation

Command parameters	Example
<code>DeviceID.exe [-m]</code> <code>[Volume] [Regex]</code>	<code>DeviceID.exe -m E:\</code> <code>"USBSTOR\DISK&amp;VEN_UFD&amp;PROD_USB_FLASH_DRIVE&amp;REV_1100\.*"</code> <p><b>Note:</b> The regex string needs to be inside quotation marks.</p>
Returns	<b>Match!</b> or <b>Not match!</b>

# Index

## A

- AddDefaultHeader field 819
- AddDefaultPassHeader field 820
- administration
  - introduction to 45
- administration console
  - about 46
  - logging on and off 47
- Administrator account
  - about 48
  - email account 50
  - password, changing 49
- administrator\_password parameter 259
- Advanced Process Control 150
- advanced server settings 807
- AES keys 255
- Agent configuration
  - about 1081
  - adding 1082
  - applying 1087
- agent events
  - about 1124
  - filter options 1125
- agent overview
  - actions 1122
  - agent overview screen 1117
- AgentInstall.msi package 1108
- alerts. *See* system alerts
- AllowHosts field 822, 835
- application monitoring 1056
  - about 1131
  - adding an application 1132
- authentication credentials 99
- authentication key 1106

## B

- BindAddress field 822, 835
- blocking requests 836
- Blue Coat ProxySG 833
- BoxMonitor process 226

## C

- CA certificates
  - importing 168
- CD/DVD
  - about 1054
- certificates
  - server, generating 262
  - sslkeytool 260, 262
- character encoding 266
- checksum offloading 805
- Classification Server
  - configuring 164
- clipboard 1056
- code numbers
  - system events 119
- comma-separated values 268
- console. *See* administration console
- create\_error\_file property 268
- credential store
  - adding authentication 100
  - deleting credentials 101
  - editing credentials 101
  - endpoint credentials 100
  - managing 101
- credentials 99
- custom attributes 797
  - creating 799
  - editing 799
  - setting values for remediation 799
  - using 797

## D

- dashboard reports
  - creating 750
- dashboards 748
  - deleting 759
  - editing 758
  - viewing 749
- Data Classification for Enterprise Vault
  - about 41

**Data Identifiers**

- about 416
  - Content Matches Data Identifier condition 434
  - creating 441
  - cross-component matching 425
  - custom script validators, about 426
  - custom, about 429
  - modifying 441
  - modifying, about 425
  - optional validators, about 421
  - optional validators, configuration 440
  - optional validators, acceptable characters 422
  - system-defined 417
  - validators, about 426
  - validators, available 426
- Data Identifiers, about
- breadths 420
- data identifiers, about
- patterns 426
- Data Identifiers, system
- breadths, list of 436
  - normalizers, list of 436
- Data Identifiers
- configuration, about 430
- data loss prevention. *See* Symantec Data Loss Prevention
- databases
- indexing 266–268
- DBPasswordChanger utility
- example of using 259
  - introducing 254, 258
  - locating 259
  - prerequisites for using 258
  - running 259
- debug log files 225–226, 237
- deploying
- using the Endpoint FlexResponse utility 1093
- Described Content Matching (DCM)
- about 286
- detection
- CAD formats 400
  - database file formats 400
  - email formats 399
  - encapsulation formats 398
  - graphics formats 400
  - other formats 400
  - presentation formats 397
  - spreadsheet formats 398
  - text and markup formats 399

**detection (*continued*)**

- word processing formats 396
- detection servers 257
- about 150
  - adding 166
  - configuration 152
  - controls 151
  - errors and warning list 172
  - kinds of 36
  - logging 231
  - removing 167
  - Server Detail screen 172
  - server settings 174
  - settings, advanced 165
  - status of 170
  - System Overview screen 169
- detection, file name
- examples 481
- detection, file properties
- file and attachment size 480
- detection, file property
- file name 480
- Directory Group Matching (DGM)
- about 287
- Directory Group Matching (DGM), profiled
- implementation, about 523
- Directory Group Matching (DGM), synchronized
- directory server connection, about 513
  - directory server connection, create 513
  - implement, about 511
  - Recipient matches User Group based on a Directory Server Group 520
  - scheduling indexing 516
  - Sender/User matches User Group based on a Directory Server Group 519
- Directory Group Matching (DGM), synchronized
- User Group, create 517
  - User Group, modify 517
- Documentum targets 1023

**E**

- ECU. *See* Environment Check Utility
- eculogs.zip file
- contents of 258
- ECUoutput.txt file 258
- EDM indexes
- using 275
- EDMIndexDirectory folder 266

- email
  - blocking 822
  - quarantining 824
- Endace cards 806
  - configuring Network Monitor to use 808
  - drivers for 806
  - installing drivers for 807
- Endpoint
  - Quarantine response rule 1070
  - user cancel response rule 1064
- endpoint
  - agent advanced settings 204
  - incompatible detection and response rules 1062
  - policies for 1060
  - response rules in different locales 1077
  - setting response rules in different locales 1078
  - setting the endpoint location 1076
- Endpoint Discover
  - about 1049
  - adding a rule 1069
  - configuring targets 1072
  - creating a policy 1068
  - creating a policy group 1068
  - how it works 1050
  - implementing 1067
  - introducing 40
  - monitoring 1059
  - reports 1066
  - scanning a target 1071
  - target filters 1071
  - targeted scans 1060
- Endpoint FlexResponse
  - about 1089
  - deploying 1090
  - deploying plug-ins 1091
  - deploying plug-ins using the Endpoint FlexResponse utility 1093
  - enabling on Enforce Servers 1094
  - uninstalling using the FlexResponse utility 1095
- Endpoint FlexResponse utility 1092
- endpoint location
  - setting 1076
- Endpoint Prevent
  - about 1049
  - application monitoring 1056
  - block response rule 1062–1063
  - CD/DVD monitors 1054
  - clipboard monitor 1056
  - creating policies 1062
- Endpoint Prevent *(continued)*
  - how it works 1051
  - implementing 1075
  - introducing 41
  - monitoring 1052
  - network monitors 1057
  - network share monitoring 1057
  - notify response rule 1062–1063
  - print/fax monitor 1055
  - removable media 1053
  - reports 1066
- Endpoint Server
  - about 1051
  - configuration, basic 163
  - redundancy 1108
- endpoint targets
  - configuring 1072
- endpoint tools 1135
  - endpointkeytool utility 1136–1137
  - logdump.exe tool 1140
  - Service\_Shutdown.exe tool 1138
  - using on Windows Vista 1136
  - vontu\_sqlite3.exe tool 1139
- endpoint utilities 255
- endpointkeytool utility 255, 1136
- Enforce
  - introducing 37
  - logging 230
- Enforce console. *See* administration console
- Enforce Server
  - about 46
  - alerts, configuring to send 115
  - choosing a non-English language for 61
  - enabling Endpoint FlexResponse 1094
  - introducing 37
  - response rules in different locales 1077
  - setting response rules in different locales 1078
- Enforce server 257
- Enforce Server administration console
  - Profile screen 50
- Environment Check Utility
  - introducing 254, 256
  - locating 257–258
  - output of 258
  - running 257
- EnvironmentCheckUtility command 257–258
- ErrorLog.txt file 258
- ethtool 805

- Exact Data Matching (EDM)
  - about 284
  - creating the data source file 374
  - migrating legacy DOE configurations 375
  - preparing for indexing 376
  - profiling keyword dictionaries 455
- Exact Data Matching (EDM), about
  - best practices 390
  - data owner exception (DOE), about 370
  - Exact Data Profiles 372
  - field mapping 370
  - indexing schedule 371
  - match counting 371
- Exact Data Matching (EDM), configuration
  - implementation process 368
- Exact Data Matching (EDM), configure
  - Content Matches Exact Data condition, configuring 387
  - Exact Data Profile 379
  - Remote EDM Indexer 378
  - uploading the exact data source to Enforce 378
- Exact Data Matching (EDM), file encoding
  - East Asian languages, UTF-16 272
  - East Asian languages, UTF-8 encoding 272
- Exact Data Matching (EDM), file encoding
  - Latin characters, iso-8859-1 272
- Exact Data Matching (EDM), profile
  - mapping fields 384
  - schedule profile indexing 386
- Exact Data Matching (EDM), profiles
  - add 372
  - manage 372
- Exact Data Matching, about
  - implementing 368
- Exchange targets 939
- ExportEDMProfile.edm file 266

## F

- files
  - indexing 268
- filtering requests 830
- FIPS 1116
- flrinst.exe utility
  - about 1092
  - installing plug-ins 1093
  - retrieving plug-in list 1096
  - retrieving plug-ins 1095
  - uninstalling plug-ins 1095
- forwarding mode 815–816

## G

- GET commands 809, 835
- group exceptions, type
  - Recipient Matches Pattern 506
- group rules, type
  - Recipient Matches Pattern 506

## H

- HostFileLog.txt file 258
- HTTP proxies. *See* proxy servers
- HTTP requests 159
  - blocking 836
  - ignoring 829–830

## I

- ICAP 39, 829, 833, 835
  - configuring 832
- incident remediation 783
- incident reports 745
  - creating summary reports 752
  - customizing 753
  - dashboards 748, 753
  - dashboards, creating 750
  - deleting custom reports 759
  - editing custom reports 758
  - filtering 755, 761
  - implementing a strategy 747
  - remediating incidents 787
  - saving 755
  - scheduling 756
  - setting advanced filters 766
  - setting general filters 763
  - setting preferences 747
  - summaries 748, 751, 761
  - summary options 777
  - viewing incidents 786
  - viewing summary reports 752
- incidents
  - attributes, status 793
  - custom attributes 797, 799
  - remediating with custom attributes 799
- incremental scanning 882–884
- Indexed Document Matching
  - Content Matches Document Signature
    - condition 411
  - excluding content 404
  - filtering documents 408
  - preparing the document source for indexing 403

Indexed Document Matching (*continued*)  
 scheduling indexing 409  
 whitelisting 404

Indexed Document Matching (IDM)  
 adding document profiles 405  
 best practices 412  
 configuring document profiles 405  
 Document Profiles, add 400  
 Document Profiles, manage 400  
 implementing 402

Indexed Document Matching  
 implementing, about 393

Indexed Document Matching (IDM)  
 about 285  
 stopwords 533

Indexer.properties file 267  
 editing 276

indexes 266  
 using 275

installation log files 225

internationalization. *See* languages and character sets

Internet Content Adaptation Protocol. *See* ICAP  
 iptables command 820–821  
 iso-8859-1 encoding 266, 274

## J

JDBC drivers 266

## L

Language Pack Utility 62

language packs  
 about 59

Language Pack Utility 62

languages and character sets

character sets, using 58  
 choosing a non-English language 61  
 language packs, about 59  
 language packs, working with 62

licenses 135

Linux systems 820

Livelihood targets 1033

localization. *See* languages and character sets

Lock Manager service 257

Log Collection Utility  
 introducing 254

log files 225

logdump.exe tool 1140

logdump.exe utility 256

logging on and off 47

logs

review 119

Lotus Notes targets 909

## M

mail transfer agents. *See* MTAs

manager process 227

Microsoft Exchange targets 975

Microsoft ISA 833

MIME types 160, 831

minSizeofGetURL field 836

monitorSettings directory 256–257

monitorSettings folder 258

MTAResubmitPort field 819

MTAs 38, 158, 813, 815, 818  
 configuring 821

MX records 157, 817

## N

network connections

checking 257

Network Discover

adding new targets 850

configuring 847

configuring targets 855, 857

editing targets 852

how Discover works 845

how scanners work 951

incident reports 889–890

introducing 39, 843

logging 229

quarantine files 906

reports 889

setting up 847

Network Discover scans

auditing targets 869

authentication 860

deleting 888

differential scans 886

encrypting passwords 861

excluding items or repositories 861

filtering by item size 864

filtering by last-accessed date 865

filtering by modified date 865

including items or repositories 861

inventory scans 869

Network Discover scans (*continued*)

- list of targets 874
- managing 874
- monitoring 874
- optimizing 868, 880
- parallel 886
- removing targets 887
- reporting 874
- reporting scan details 876
- reporting scan history 879
- scheduling 858
- status 875
- throttling 868

## Network Discover Server

- configuration, basic 162
- configuring 848
- configuring parallel scans 886
- Linux 850

## Network Discover targets 962

- custom 1041
- DB2 databases 919
- Documentum 1023
- Domino servers 909
- Exchange 939, 975
- file shares 899
- Livelink 1033
- Lotus Notes 909
- Oracle databases 919
- removing 887
- SharePoint 927
- SharePoint 2003 1003
- SharePoint 2007 991
- SQL databases 919
- SQL server 2005 919
- UNIX file systems 962
- Web servers 1011
- Web services 1041
- Web sites 1011
- Windows remote server file systems 962

network interface card. *See* NIC

## Network Monitor

- configuring 807
- creating policies for 810
- implementing 803, 805
- introducing 38
- logging 230
- requirements for 803
- testing 810
- using Endace cards with 807

## Network Monitor Server

- configuring 154

## Network Prevent (Email)

- blocking email 822
- bouncing messages 736
- configuring 816
- creating policies for 822
- enabling policy violation headers 824
- implementing 813, 815
- integrating MTAs with 815
- introducing 38
- logging 230
- routing restricted ports to 820
- testing 825

## Network Prevent (Email) Server

- configuring 156

## Network Prevent (Web)

- configuring 829, 835
- creating policies for 836
- implementing 827, 829
- introducing 38
- testing 838
- troubleshooting 838

## Network Prevent (Web) Server

- configuring 159

## Network Protect

- introducing 40
- quarantine files 906

## Network Protect server

- configuration, basic 162
- network share monitoring 1057
- network taps 803, 805
- new\_oracle\_password parameter 259
- Next MTA field 818
- NIC 804–805
- Notification service 257

**O**

operational log files 225

Oracle database 257

- NLS\_LANGUAGE setting 61
- NLS\_TERRITORY setting 61

**P**

packet capture software 804–805

- installing 806

PACKET\_MMAP software 806

Password Renewal window 53

- password\_file parameter 259
- passwords 259
  - See also* DBPasswordChanger utility
  - Administrator 49
  - changing 50, 53, 259
  - encrypting for Network Discover scans 861
- pcapstart.reg file 807
- pdx extension 275
- plug-ins
  - deploying on the endpoint 1091
- policies
  - about 307
  - add 337
  - adding reponse rules 363
  - components 309
  - configuration 338
  - create 357
  - deployment 312
  - manage 357
  - privileges, administration 313
  - privileges, authoring 313
  - privileges, response rules 313
  - removing 364
  - solution pack 311
- policies, about
  - best practices 318
  - Data Profiles 316
  - implementation 317
  - User Groups 317
- policy conditions
  - Content Matches Data Identifier 434
- policy detection
  - false negatives, about 302
  - false positives, about 302
  - introducing 281
- policy detection template, configuration
  - Yahoo Message Board 672
- policy detection templates, configuration
  - Caldicott Report 603
  - CAN-SPAM Act 605
  - Canadian Social Insurance Numbers 605
  - Common Spyware Upload Sites 607
  - Competitor Communications 607
  - Confidential Documents 608
  - Credit Card Numbers 609
  - Customer Data Protection 609
  - Defense Message System (DMS) GENSER
    - Classification 613
  - Design Documents 615
  - policy detection templates, configuration *(continued)*
    - Employee Data Protection 616
    - Encrypted Data 617
    - EU Data Protection Directives 612
    - Export Administration Regulations (EAR) 618
    - FACTA 2003 (Red Flag Rules) 619
    - Financial Information 623
    - Forbidden Websites 624
    - Gambling 624
    - Gramm-Leach-Bliley 625
    - HIPAA and HITECH (including PHI) 627
    - Human Rights Act 1998 631
    - Illegal Drugs 632
    - Individual Taxpayer Identification Numbers (ITIN) 633
    - International Traffic in Arms Regulations (ITAR) 633
    - Media Files 634
    - Merger and Acquisition Agreements 635
    - NASD Rule 2711 and NYSE Rules 351 and 472 637
    - NASD Rule 3010 and NYSE Rule 342 638
    - NERC Security Guidelines for Electric Utilities 640
    - Network Diagrams 642
    - Network Security 643
    - Offensive Language 643
    - Office of Foreign Assets Control (OFAC) 644
    - OMB Memo 06-16 and FIPS 199 Regulations 646
    - Password Files 647
    - Payment Card Industry (PCI) Data Security Standards 648
    - PIPEDA 649
    - Price Information 651
    - Project Data 652
    - Proprietary Media Files 652
    - Publishing Documents 653
    - Racist Language 654
    - Restricted Files 654
    - Restricted Recipients 655
    - Resumes 655
    - Sarbanes-Oxley 656
    - SEC Fair Disclosure Regulation 658
    - Sexually Explicit Language 660
    - Source Code 661
    - State Data Privacy 662
    - SWIFT Codes 666
    - Symantec DLP Awareness and Avoidance 666
    - UK Data Protection Act 1998 611

- policy detection templates, configuration *(continued)*
  - UK Drivers License Numbers 667
  - UK Electoral Roll Numbers 667
  - UK National Health Service (NHS) Number 668
  - UK National Insurance Numbers 668
  - UK Passport Numbers 669
  - UK Tax ID Numbers 669
  - US Intelligence Control Markings (CAPCO) and DCID 1/7 669
  - US Social Security Numbers 671
  - Violence and Weapons 671
  - Webmail 671
- policy detection, about
  - appropriate use 303
  - binary content 285
  - content 281
  - cross-component matching 293
  - Data Classification for Enterprise Vault 41
  - Described Content Matching (DCM) 286
  - Directory Group Matching (DGM) 287
  - document content matching 285
  - endpoint events 283
  - engine execution logic 297
  - Exact Data Matching (EDM) 284
  - file types 282
  - getting started 301
  - identities 283
  - implementation 299
  - Indexed Document Matching (IDM) 285
  - keyword matching 449
  - languages 283
  - message components 293
  - network 282
  - precise results 301
  - profiled DGM 287
  - rule severity 295
  - strategy 300
  - synchronized DGM 287
  - technologies 283
  - two-tier 317
  - unstructured data 285
  - using compound rules 305
  - using exceptions 304
- policy detection, best practices
  - Directory Group Matching, profiled 527
  - identity pattern matching 508
  - keyword matching 456
  - regular expressions 460
- policy detection, conditions
  - content 289
  - Content Matches Document Signature 411
  - Content Matches Exact Data (EDM) 387
  - Content Matches Keyword 452
  - Content Matches Regular Expression 457
  - Custom File Type Signature 485
  - Endpoint Device Class or ID 498
  - Endpoint Location 499
  - endpoint matching 291
  - file property matching 290
  - groups 292
  - identity 292
  - Message Attachment or File Name Match 483
  - Message Attachment or File Size Match 482
  - Message Attachment or File Type Match 481
  - network protocol matching 291
  - Protocol Monitoring 488
  - Protocol or Endpoint Monitoring 493
  - Recipient Matches Directory From Exact Data
    - Profile condition 526
  - Recipient matches User Group based on a
    - Directory Server Group 520
  - Sender/User Matches Directory From Exact Data
    - Profile condition 525
  - Sender/User Matches Pattern 504
  - Sender/User matches User Group based on a
    - Directory Server Group 519
- policy detection, configuration
  - select message components to match on 348
- policy detection, custom file type
  - enabling the method 484
- policy detection, customization
  - about 287
- policy detection, described identities
  - about 503
  - Sender/User Matches Pattern 504
- policy detection, endpoint
  - destination, about 492
  - devices, about 492
  - devices, add 496
  - devices, adding 497
  - devices, configuring 497
  - devices, manage 496
  - Endpoint Device Class or ID 498
  - Endpoint Location 499
  - implementing, about 491
  - locations, about 493
  - Protocol or Endpoint Monitoring 493

- policy detection, endpoint *(continued)*
  - protocol, about 492
- policy detection, exceptions
  - types 288
- policy detection, file name
  - Message Attachment or File Name Match 483
- policy detection, file properties
  - detectable file types 465
  - file type detection 464
  - implementing 463
- policy detection, file property
  - best practices 486
- policy detection, file size
  - Message Attachment or File Size Match 482
- policy detection, file type
  - Custom File Type Signature 485
  - Message Attachment or File Type Match 481
- policy detection, file types
  - custom 479
- policy detection, international
  - about 529
  - data identifiers 531
  - document content 533
  - find keywords 531
- policy detection, keyword matching
  - exmaples 451
  - implementing 449
  - profiling keyword dictionaries 455
  - wildcards, about support for 449
- policy detection, keyword matching, configuration
  - Content Matches Keyword 452
- policy detection, keyword proximity
  - about 450
- policy detection, network
  - implementing 487
  - Protocol Monitoring 488
- policy detection, profiled DGM
  - create exact data source file 524
  - Recipient Matches Directory From Exact Data
    - Profile condition 526
  - Sender/User Matches Directory From Exact Data
    - Profile condition 525
- policy detection, profiled Directory Group Matching
  - implementation, about 523
- policy detection, regular expressions
  - Content Matches Regular Expression 457
  - implementing 457
  - writing 459
- policy detection, rules
  - compound, about 297
  - simple, about 297
  - types 288
- policy exceptions
  - about 296
  - add 349
  - compound 354
  - configure 351
- policy exceptions, configure
  - match counting 346
- policy groups
  - about 311
  - create 359
  - default policy group 311
  - deployment 312
  - managing 360
  - modify 359
  - removing 364
- policy rules
  - compound 354
- policy rules, conditions
  - configure 342
- policy rules, configuration
  - rule severity 345
- policy rules, configure
  - match counting 346
- policy rules, detection
  - add 340
- policy rules, group
  - add 340
- policy templates
  - add 337
  - create policy from 321
  - Customer and Employee Data Protection 327
  - export 314, 362
  - export from v10 362
  - import 314, 361
  - import to v11 362
  - system-defined 310
  - UK and International Regulatory
    - Enforcement 327
  - US Regulatory Enforcement 324
- policy templates, configure
  - Exact Data Profile, select 333
  - Indexed Document Profile, select 334
- policy templates, international
  - about 530

- policy templates, type
  - Confidential or Classified Data Protection 329
  - Network Security Enforcement 330
  - Yahoo and MSN Messengers on Port 80 674
- policy templates, types
  - Acceptable Use Enforcement 331
- policy violation headers 824
  - enabling 824
- print/fax 1055
- processGets field 836
- product suite. *See* Symantec Data Loss Prevention
- profiles 266, 274
- ProtectInstaller\_10.5.exe file 270
- proxy servers 827
  - compatibility with 833
  - configuring 832–833, 835

## Q

- quarantine files 906
- queries 266

## R

- rdx extension 275
- reflecting mode 815–816
- remediation 783
- Remote EDM Indexer utility
  - command-line options for 274
  - creating EDM profile with 271
  - example use of 275
  - installing 269–270
  - introducing 255, 268
  - requirements for using 268
  - running 269–271, 274–276
  - running SQL Preindexer with 265
  - troubleshooting 276
  - uninstalling 277
- response rules, conditions
  - incident type 705
  - severity 711
- Reporting API 85
- Reporting API Web Service 228
- reports 745
  - dashboards 748
  - summaries 751
  - system events 104
- REQMOD 832–833
- RequestProcessor settings 824
- RequestProcessor fields 819, 822, 825

- RESPMOD 832–833
- response filtering 831
- response rules
  - about 680
  - add 695
  - best practices 692
  - configure 697
  - manage 695
  - modify ordering 701
- response rules, about
  - actions 680
  - authoring privileges 690
  - automated 686
  - conditions 687
  - execution 685
  - execution priority for actions 688
  - implementation 691
  - removing 702
  - Smart 686
  - Smart, configure 698
- response rules, actions
  - Add Note 714
  - configure 699
  - discarding network incident data 716
  - Endpoint Discover: Quarantine File 722
    - See also*
  - Endpoint Prevent Block 725
  - Endpoint Prevent Notify, configuration 728
  - Endpoint Prevent User Cancel,
    - configurations 731
  - Endpoint: FlexResponse 721
  - Limit Incident Data Retention 714
  - Log to a Syslog Server 717
  - Network Prevent Block FTP Request 734
  - Network Prevent Block HTTP/S 734
  - Network Prevent: Block SMTP Message 736
  - Network Prevent: Modify SMTP Message 737
  - Network Prevent: Remove HTTP/HTTPS
    - Content 738
  - Network Protect Copy File 740
  - Network Protect Quarantine File,
    - configuration 740
  - retaining endpoint incident data 715
  - Send Email Notification 718
  - Set Attribute 720
  - Set Status 721
- response rules, adding
  - Automated 697
  - Smart 697

- response rules, conditions
  - configure 698
  - endpoint device 704
  - endpoint location 703
  - incident match count 707
  - protocol or endpoint monitoring 708
- response rules, type
  - Endpoint Prevent Block 1063
  - Endpoint Prevent Notify 1063
  - Endpoint Prevent User Cancel 1064
  - Endpoint Quarantine 1070
- response rules, types
  - all detection servers 681
  - classification 684
  - endpoint 682
  - network 683
- restricted ports 819–820
- roles
  - add 91
  - adding 82
  - configuring 82
  - manage 91
- roles, about
  - configuring 78
  - recommended 79
  - role-based access control 77
  - solution pack, included with 80
- RRC. *See* rules results caching
- rules results caching 1065

## S

- scans
  - differential scans 882
  - incremental scans 882–884
- Secure Computing Secure Web 833
- separator characters 267
- Server Detail screen 172
  - server configuration 152
- servers (DLP). *See* detection servers and Enforce Server
- ServerSocketPort field 819
- Service\_Shutdown.exe tool 1138
- Service\_Shutdown.exe utility 256
- services 256
- SharePoint 2003 targets 1003
- SharePoint 2007 targets 991
- SharePoint targets 927
- SMTP 822
- SOAP messages 228
- SOAP requests 85
- SPAN 803, 805
- SQL 256, 266
- SQL Preindexer utility
  - command-line options for 266–267
  - introducing 255, 265
  - locating 265
  - running Remote EDM Indexer with 265
  - troubleshooting 267
- Squid Web Proxy 833
- SSL certificates
  - importing 168
- sslkeytool 260
  - generating server certificates 262
  - options 261
- sslkeytool utility
  - introducing 254
- status attributes 793
- status groups
  - adding 796
  - configuring 796
  - deleting 796
- status values
  - adding 795
  - configuring 795
  - deleting 795
- Switch Port Analyzer. *See* SPAN
- Symantec Data Loss Prevention
  - administration of 45
  - initial system setup 48
  - product suite 35
- Symantec Data Loss Prevention servers. *See* detection servers and Enforce Server
- Symantec DLP Agent
  - about 1052
  - administration 1117
  - advanced settings 204
  - AgentInstall.msi package 1108
  - authentication key 1106
  - installation 1102
  - installed aspects 1103
  - installing manually 1114
  - installing on Windows Vista 1104
  - installing with FIPS compliant machines 1116
  - installing with Symantec Management Console 1111
  - installing with system management software 1112
  - preinstallation steps 1104

- Symantec DLP Agent (*continued*)
  - removing 1126
  - removing manually 1130
  - removing on Windows Vista 1129
  - removing with Symantec Management Console 1127
  - removing with system management software (SMS) 1128
  - security 1105
  - watchdog service 1107
- Symantec Management Agent
  - installing 1099
- Symantec Management Console 1097
  - agent tasks 1101
  - cloning advertisements and programs 1098
  - creating user tasks 1102
  - reporting 1100
  - Symantec Management Agent 1099
  - using computer discovery 1098
- syslog servers 113
- system accounts 257
- system alerts
  - about 115
  - adding 117
  - configuring server 115
  - modifying 117
- System Center Configuration Manager 1112
- system events 103
  - code numbers 119
  - event details 108
  - notification methods 104
  - reports 104
  - reports, filtering 105
  - reports, saved 107
  - responses 111
  - syslog servers 113
  - thresholds, configuring 109
  - types (severities) of 108
- System Overview screen 169
  - detection server, adding 166
  - errors and warning list 172
  - server status 170
- system setup, initial 48
- system upgrades 136
- Systems Management Server (SMS) 1112

## T

- tab-delimited files 268
- TagHighestSeverity field 825

- TagPolicyCount field 825
- TagScore field 825
- telnet command 821
- TLS proxies 157, 820
- trial mode 157, 816, 829

## U

- upgrades, system 136
- user agents 830
- users
  - add 92
  - manage 92
- users, about
  - configuring 78
- users, accounts
  - adding 89
  - configuring 89
- users, authentication
  - Active Directory 92
  - configuring Enforce for Active Directory authentication 96
  - integrating Enforce with Active Directory 93
  - verifying the Active Directory connection 95
- users, passwords
  - configuring strong or rotating 90
- UTF-16 encoding 266, 274
- UTF-8 encoding 266, 274
- utilities
  - introducing 253, 255

## V

- Vector Machine Learning (VML)
  - stopwords 533
- violated policies 824
- Vontu services
  - starting 70–75
  - stopping 70–75
- vontu\_sqlite3.exe tool 1139
- vontu\_sqlite3.exe utility 256

## W

- watchdog service 1107
- Web Services 85
- Webwasher 833
- WinPcap software 805–806
  - installing 806

**X**

- X-Filter-Loop: Reflected header 820
- X-DLP-Max-Severity header 825
- X-DLP-Policy-Count header 825
- X-DLP-Score header 825