Symantec™ Data Loss Prevention System Requirements and Compatibility Guide

Version 11.6

Last updated: 13 September, 2012

Symantec

Symantec Data Loss Prevention System Requirements and Compatibility 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.

Document version: 11.6d

Legal Notice

Copyright © 2012 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/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

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/

Select your country or language from the site index.

Contents

Chapter 1

System Requirements and Recommendations

This chapter includes the following topics:

About updates to Symantec Data Loss Prevention system requirements

System requirements as described in this guide are occasionally updated as new information becomes available. You can find the latest version of the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* at the following link to the Symantec Data Loss Prevention knowledgebase. You must be a licensed Symantec Data Loss Prevention customer and have a login for the knowledgebase to access this article.

https://kb-vontu.altiris.com/article.asp?article=55645

Table 1-1 Change log

Date	Description
13 September, 2012	Updated supported versions of Symantec Data Insight. See "Data Insight compatibility with Symantec Data Loss Prevention version 11.x" on page 43. Added supported versions of Microsoft Active Directory. See "Third-party software requirements and recommendations" on page 35. Added supported versions of McAfee Web Gateway. See "Proxy server compatibility with Network Prevent for Web" on page 40. Updated supported versions of Symantec Veritas Cluster Server (VCS). See "Symantec / Symantec Data Loss Prevention integrations" on page 44.

About accessing the Symantec Data Loss Prevention Knowledgebase

In addition to your product documentation, the Symantec Data Loss Prevention Knowledgebase is a valuable resource for information. The Knowledgebase provides solutions to common problems, troubleshooting tips, and other useful information. In addition, important product announcements, updated release notes and product guides, and product bulletins are published at the Knowledgebase.

The Knowledgebase is available at https://kb-vontu.altiris.com.

You must create an account with a user name and password to access the Knowledgebase. All Data Loss Prevention users are strongly encouraged to create a Knowledgebase account.

To create an account

1. Navigate to the Knowledgebase login page at https://kb-vontu.altiris.com.
2. Click the **New User** link to request access.

It may take several days to process your request.

Deployment planning considerations

Installation planning and system requirements for Symantec Data Loss Prevention depend on:

- The type and amount of information you want to protect
- The amount of network traffic you want to monitor
- The size of your organization
- The type of Symantec Data Loss Prevention detection servers you choose to install

These factors affect both:

- The type of installation tier you choose to deploy (three-tier, two-tier, or single-tier)
  See "About installation tiers" on page 13.
- The system requirements for your Symantec Data Loss Prevention installation

See "The effect of scale on system requirements" on page 14.

About installation tiers

Symantec Data Loss Prevention supports three different installation types: three-tier, two-tier, and single-tier. Symantec recommends the three-tier installation. However, your organization might need to implement a two-tier installation depending on available resources and organization size. Single-tier installations are recommended only for performing risk assessments or testing the software.

Single-tier	To implement the single-tier installation, you install the database, the Enforce Server, and a detection server all on the same computer. Use single-tier installation only for testing or risk assessment purposes.

Two-tier	To implement the two-tier installation, you install the Oracle database and the Enforce Server on the same computer. You then install detection servers on separate computers. Typically, this installation is implemented when an organization, or the group responsible for data loss prevention, does not have a separate database administration team. If you choose this type of installation, the Symantec Data Loss Prevention administrator needs to be able to perform database maintenance tasks, such as database backups. See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 15.
Three-tier	To implement the three-tier installation, you install the Oracle database, the Enforce Server, and a detection server on separate computers. Symantec recommends implementing the three-tier installation architecture as it enables your database administration team to control the database. In this way you can use all of your corporate standard tools for database backup, recovery, monitoring, performance, and maintenance. Three-tier installations require that you install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server to communicate with the Oracle server. See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 15.

The effect of scale on system requirements

Some system requirements vary depending on the size of the Symantec Data Loss Prevention software deployment. Determine the size of your organization and the corresponding Symantec Data Loss Prevention deployment using the information in this section.

The key considerations in determining the deployment size are as follows:

- Number of employees to be monitored
- Amount of network traffic to monitor
- Size of Exact Data Match profile (EDM) or Indexed Data Match profile (IDM)

The following table outlines two sample deployments based on enterprise size. Review these sample deployments to understand which best matches your organization's environment.

Table 1-2 Types of enterprise deployments

Variable	Small/Medium Enterprise	Large/Very Large Enterprise
Number of employees	< 10,000	> 10,000
Volume of network traffic to monitor	30–40 Mbps	> 40 Mbps
EDM/IDM size	EDM < 1 million cells or IDM < 1,000 pages	EDM > 1 million cells or IDM > 1,000 pages
Hardware requirements	See "Small/medium enterprise minimum hardware requirements" on page 16.	See "Large/very large enterprise minimum hardware requirements" on page 17.

For additional related information see also *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines.*

Minimum system requirements for Symantec Data Loss Prevention servers

All Symantec Data Loss Prevention servers must meet or exceed the minimum hardware specifications and run on one of the supported operating systems.

- See "Small/medium enterprise minimum hardware requirements" on page 16.
- See "Large/very large enterprise minimum hardware requirements" on page 17.
- See "Operating system requirements for servers" on page 18.

New installations of Symantec Data Loss Prevention version 11 require Oracle 11g to store the Enforce Server database. You cannot install a new Symantec Data Loss Prevention version 11 Enforce Server using an existing Oracle 10g database.

If you are upgrading an earlier version of Symantec Data Loss Prevention to version 11, you can continue to use your existing Oracle10g database. After upgrading to Symantec Data Loss Prevention version 11, you should upgrade to Oracle 11g to receive continued security updates.

If the Oracle database is installed on a dedicated computer (a three-tier deployment), that system must meet it own set of system requirements.

See "Oracle database requirements" on page 27.

Symantec Data Loss Prevention installations that include the Endpoint Discover or Endpoint Prevent products can optionally use a separate Symantec Management Platform installation to manage Symantec DLP Agents on endpoint computers. Symantec Management Platform is a separate product and has its own set of

system requirements, and only certain versions are supported for managing Symantec DLP Agents.

See "About Symantec Management Platform server requirements" on page 27.

Small/medium enterprise minimum hardware requirements

The following table provides the system requirements for small and medium-size enterprise systems.

Table 1-3 Small/medium enterprise minimum system requirements

Required for	Enforce Server	Network Monitor	Network Discover, Network Prevent, Mobile Prevent for Web, Endpoint Prevent, or Classification server
Processor	2 x 3.0 GHz CPU	2 x 3.0 GHz CPU	2 x 3.0 GHz CPU
Memory	6–8 GB RAM (EDM/IDM size can increase memory requirements) Two-tier deployments may require additional memory for running Oracle.	6–8 GB RAM (EDM/IDM size can increase memory requirements)	6–8 GB RAM (EDM/IDM size can increase memory requirements)
Disk Requirements	500 GB, RAID 1+0 or RAID 5 configuration is recommended For Network Discover deployments, appoximately 150 MB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target.	140 GB	140 GB For Network Discover deployments, appoximately 150 MB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target.
NICs	1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with detection servers.	1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with the Enforce Server.	1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with the Enforce Server.

See "Oracle database requirements" on page 27.

See "The effect of scale on system requirements" on page 14.

Large/very large enterprise minimum hardware requirements

The following table provides the system requirements for large and very large enterprise systems.

Table 1-4 Large/Very Large enterprise minimum system requirements

Required For	Enforce Server	Network Monitor	Network Discover, Network Prevent, Mobile Prevent for Web, Endpoint Prevent, or Classification Server
Processor	2 x 3.0 GHz Dual Core CPU	2 x 3.0 GHz Dual Core CPU	2 x 3.0 GHz Dual Core CPU
Memory	8–16 GB RAM (EDM/IDM size can increase memory requirements) Two-tier deployments require additional memory for running Oracle.	8–16 GB RAM (EDM/IDM size can increase memory requirements)	8–16 GB RAM (EDM/IDM size can increase memory requirements)
Disk Requirements	1 TB, RAID 1+0 or RAID 5 configuration is recommended For Network Discover deployments, appoximately 1 GB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target.	140 GB	140 GB For Network Discover deployments, appoximately 1 GB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target.

Table 1-4 Large/Very Large enterprise minimum system requirements *(continued)*

Required For	Enforce Server	Network Monitor	Network Discover, Network Prevent, Mobile Prevent for Web, Endpoint Prevent, or Classification Server
NICs	To communicate with detection servers: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC	To communicate with the Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet For network traffic monitoring (pick one): 1 copper or fiber 1 Gb/100 Mb Ethernet NIC.	To communicate with the Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC
High-speed packet capture cards	n/a	See "High-speed packet capture cards" on page 42.	n/a

See "Oracle database requirements" on page 27.

See "The effect of scale on system requirements" on page 14.

Operating system requirements for servers

Symantec Data Loss Prevention servers can be installed on a supported Linux or Windows operating system. Different operating systems can be used for different servers in a heterogeneous environment. (The Classification detection server, used with the Data Classification for Enterprise Vault product, is not supported on Linux operating systems.)

Symantec Data Loss Prevention supports the following operating systems for Enforce Server and detection server computers:

- Microsoft Windows Server 2003 SP2, Enterprise Edition (32-bit)
- Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit)
- Microsoft Windows Server 2008 R2, Standard Edition (64-bit)
- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition (64-bit)
- Microsoft Windows Server 2008 R2 SP1, Standard Edition (64-bit)
- Red Hat Enterprise Linux 5.2 through 5.8 (32-bit)
- Red Hat Enterprise Linux 5.2 through 5.8 (64-bit)

Note: Support for 32-bit platforms for the Enforce Server and for detection servers will be discontinued in a future version of Symantec Data Loss Prevention. Symantec recommends that customers migrate to 64-bit systems as soon as possible.

English language versions of both operating systems are supported. In addition, localized versions of Windows platforms are supported for Symantec Data Loss Prevention servers and endpoint computers. Localized versions of Linux platforms are supported only for Symantec Data Loss Prevention servers.

See "Supported languages for detection" on page 23.

See also the *Symantec Data Loss Prevention Administration Guide* for detailed information about supported languages and character sets.

See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 15.

Linux partition guidelines

Minimum free space requirements for Linux partitions vary according to the specific details of your Symantec Data Loss Prevention installation. The table below provides general guidelines that should be adapted to your installation as circumstances warrant. Symantec recommends using separate partitions for the different file systems, as indicated in the table. If you combine multiple file systems onto fewer partitions, or onto a single root partition, make sure the partition has enough free space to hold the combined sizes of the file systems listed in the table.

Note: Partition size guidelines for detection servers are similar to those for Enforce Server without an Oracle database.

See Table 1-6 on page 20.

Table 1-5 Linux partition minimum size guidelines—Enforce Server with Oracle database

Partition	Minimum free space	Description and comments
`/home`	6 GB	Store the Oracle installation tools, Oracle installation ZIP files, and Oracle critical patch update (CPU) files in `/home`.
`/tmp`	1.2 GB	The Oracle installer and installation tools require space in this directory.

Table 1-5 Linux partition minimum size guidelines—Enforce Server with Oracle database *(continued)*

Partition	Minimum free space	Description and comments
`/opt`	500 GB for Small/Medium installations 1 TB for Large/Very Large installations	Contains installed programs such as Symantec Data Loss Prevention, the Oracle Server, and the Oracle database. The Oracle database requires significant space in this directory. For improved performance, you may want to mount this partition on different disks/SAN/RAID from where the root partition is mounted.
`/var`	15 GB for Small/Medium installations 46 GB for Large/Very Large installations	Contains logs, EDM/IDM indexes, incremental scan indexes, and network packet capture directories. **Note:** The `/var/spool/pcap` and `/var/vontu/drop_pcacp` directories must reside on the same partition or mount point.
`/boot`	100 MB	This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported).
swap	Equal to RAM	If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts.

Table 1-6 Linux partition minimum size guidelines—Enforce Server without a database, or detection server

Partition	Minimum size guidelines	Description and comments
`/opt`	10 GB	Contains installed programs such as Symantec Data Loss Prevention and the Oracle client.
`/var`	15 GB for Small/Medium installations 46 GB for Large/Very Large installations	Contains logs, EDM/IDM indexes, incremental scan indexes, and network packet capture directories. **Note:** The `/var/spool/pcap` and `/var/vontu/drop_pcacp` directories must reside on the same partition or mount point.
`/boot`	100 MB	This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported).

Table 1-6 Linux partition minimum size guidelines—Enforce Server without a database, or detection server *(continued)*

Partition	Minimum size guidelines	Description and comments
swap	Equal to RAM	If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts.

Endpoint computer requirements for the Symantec DLP Agent

If you install Endpoint Prevent, the endpoint computers on which you install the Symantec DLP Agent must meet the requirements that are described in the following sections.

- See "Operating system requirements for endpoint systems" on page 21.
- See "Memory and disk space requirements for the Symantec DLP Agent" on page 22.
- See "Symantec DLP Agent connectivity requirements" on page 22.

Operating system requirements for endpoint systems

Symantec DLP Agents can be installed on computers running any of the following Windows operating systems:

- Microsoft Windows Server 2003 (32-bit) with Service Pack 2 or Windows Server 2003 R2 (32-bit)
- Microsoft Windows XP Professional with Service Pack 2 or Service Pack 3 (32-bit)
- Microsoft Windows Vista Enterprise or Business with Service Pack 1 or Service Pack 2 (32-bit)
- Microsoft Windows 7 Enterprise, Professional, or Ultimate, including Service Pack 1 (32-bit or 64-bit)
- Microsoft Windows 2008 Enterprise R2 (64-bit)

Symantec DLP Agents can also be installed on supported localized versions of these Windows operating systems.

See "Supported languages for detection" on page 23.

See also the *Symantec Data Loss Prevention Administration Guide* for detailed information about supported languages and character sets.

See "About Endpoint Data Loss Prevention compatibility" on page 52.

See "About Symantec Management Platform server requirements" on page 27.

Memory and disk space requirements for the Symantec DLP Agent

The Symantec DLP Agent software reserves a minimum of 25 MB to 30 MB of memory on the Endpoint computer, depending on the actual version of the software. The DLP Agent software temporarily consumes additional memory while it detects content or communicates with the Endpoint Prevent server. After these tasks are complete, the memory usage returns to the previous minimum.

The initial Symantec DLP Agent installation consumes approximately 70 MB to 80 MB of hard disk space. The actual minimum amount depends on the size and number of policies that you deploy to the endpoint computer. Additional disk space is then required to temporarily store incident data on the endpoint computer until the Symantec DLP Agent sends that data to the Endpoint Prevent server. If the endpoint computer cannot connect to the Endpoint Prevent server for an extended period of time, the Symantec DLP Agent will continue to consume additional disk space as new incidents are created. The disk space is freed only after the agent software reconnects to the Endpoint Prevent server and transfers the stored incidents.

Symantec DLP Agent connectivity requirements

As part of regular operation, a Symantec DLP Agent requires a persistent connection to a single Endpoint Server. This connection may remain idle for long periods of time. If the connection is broken and reestablished, or if the DLP Agent is connected to a different Endpoint Server, significant overhead is incurred while the server retransmits configured policies to the agent. For this reason, any network interfaces that reside between DLP Agents and Endpoint Servers must support persistent connections that maintain each agent's affinity to its currently connected Endpoint Server.

DLP Agents can be configured to fail over to another Endpoint Server if the current server cannot be reached. This failover process also incurs the overhead of retransmitting policies to the agent. See the *Symantec Data Loss Prevention System Adminitration Guide* for information about configuring Endpoint Server redundancy.

Symantec Data Loss Prevention for Mobile requirements

The following table contains requirements you need to set up Symantec Data Loss Prevention for Mobile (Mobile Prevent). If there are multiple options available for a requirement, each option is listed.

Note: The Symantec Data Loss Prevention Mobile Prevent for Web detection server is not supported in a virtual or hosted environment.

For system requirements for Mobile Prevent for Web detection servers:

- See "Small/medium enterprise minimum hardware requirements" on page 16.
- See "Large/very large enterprise minimum hardware requirements" on page 17.

Table 1-7 Mobile Prevent requirements

Requirement	Description
Supported devices	iPad 2, iPad (2012 version) iPhone 4, iPhone 4S (all models and carriers)
Operating systems	iOS for iPad: 4.3.x, 5.0, 5.0.1, 5.1, 5.1.1 iOS for iPhone: 5.0, 5.0.1, 5.1, 5.1.1
ActiveSync	(Required only for detection of corporate email) Microsoft Exchange 2003 and 2007 with ActiveSync
Web proxy	Blue Coat Proxy SG version 5.5.3.1 for Mobile Prevent, or for Mobile Prevent deployed with Network Prevent for Web **Note:** Your proxy server must not use network address translation (NAT) where it is located in your infrastructure.
VPN server	Cisco ASA series Cisco AnyConnect Juniper SA series

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 1-8 Languages supported by Symantec Data Loss Prevention

Language	Version 9.x	Version 10.0	Version 10.5	Versions 11.0, 11.1.x, 11.5, 11.6
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
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

Table 1-8 Languages supported by Symantec Data Loss Prevention *(continued)*

Language	Version 9.x	Version 10.0	Version 10.5	Versions 11.0, 11.1.x, 11.5, 11.6
Turkish		Yes*	Yes*	Yes*

Languages supported by Symantec Data Loss Prevention Versions 10.5, 11.0, 11.1, 11.5, 11.6

*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.

Available language packs

You can install any of the available language packs for your Symantec Data Loss Prevention deployment. Language packs provide a limited set of non-English languages for the Enforce Server administration console user interface and online Help. Note that these language packs are only needed to provide a translated user interface and online Help; they are not needed for data detection. Language packs also contain translated versions of selected Symantec Data Loss Prevention documentation.

As they become available, language packs for Symantec Data Loss Prevention are distributed along with the software products they support. You can also download and add a language pack to an installation. Language packs do not require any additional purchase or license. Consult the *Symantec Data Loss Prevention Administration Guide* for details on how to add and enable a language pack. Language packs are distributed as downloadable files on the Symantec FileConnect Web site with file names in the form:

`Symantec_DLP_11.6_Lang_Pack_`*`language`*`.zip`

Language packs are available for the following languages:

Language	Locale code
Brazilian Portuguese	`PT_BR`
Chinese (Simplified)	`ZH_CN`
Chinese (Traditional)	`ZH_TW`
French	`FR_FR`
Japanese	`JA_JP`
Korean	`KO_KR`
Mexican Spanish	`ES_MX`

Language	Locale code
Russian	RU_RU

Note: Not all language packs are available when a product is first released.

About Symantec Management Platform server requirements

Installations that include the Endpoint Discover or Endpoint Prevent products can optionally use Symantec Management Platform 7.0 (MR4 or later) or, as of Symantec Data Loss Prevention version 11.1.1, Symantec Management Platform 7.1 (SP0 or later) to manage Symantec DLP Agents. Symantec Management Platform 7.0 MR4 or 7.1 is required to support Windows 7 endpoint computers.

Altiris 6 users must upgrade to Symantec Management Platform 7.x and migrate existing management data. The Symantec Management Platform performs automated asset discovery and endpoint installation of the Symantec DLP Agents.

Note: Installing and using the Symantec Management Platform with Symantec Data Loss Prevention is optional. However, the Symantec Management Platform offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention. For example, you can use the Symantec Management Platform to find and manage all of the endpoint computers in your organization, or troubleshoot Symantec DLP Agents installed on endpoint computers. See the *Symantec Data Loss Prevention Administration Guide* for more information.

See the *Symantec Management Platform Installation Guide* for more details about Symantec Management Platform requirements and installation options.

Oracle database requirements

All new Symantec Data Loss Prevention installations must install and use Oracle 11g version 11.2.0.3 (32-bit or 64-bit) with the most recent Critical Patch Update. Symantec Data Loss Prevention includes Oracle 11g and the necessary patches.

You cannot install a new Symantec Data Loss Prevention version 11 Enforce Server with an Oracle 10g database.

If you are upgrading an earlier version of Symantec Data Loss Prevention to version 11, you can continue to use your existing Oracle10g database version

10.2.0.4 (32-bit only) with the most recent Critical Patch Update. Oracle 10g is not supported on 64-bit operating systems. After upgrading to Symantec Data Loss Prevention version 11, you should upgrade to Oracle 11g to receive continued security updates. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for information about installing or upgrading Oracle software.

Symantec Data Loss Prevention requires the Oracle database to use the AL32UTF8 character set. If your database is configured for a different character set, the installer notifies you and cancels the installation.

You can install Oracle on a dedicated server (a three-tier deployment) or on the same computer as the Enforce Server (a two-tier or one-tier deployment):

- Three-tier deployment.
  System requirements for a dedicated Oracle server are listed below. Note that dedicated Oracle server deployments also require that you install the Oracle 11g Client on the Enforce Server computer to communicate with the remote Oracle 11g instance.
- One- and two-tier deployments.
  When installed on the Enforce Server computer, the Oracle system requirements are the same as those of the Enforce Server.
  See "Small/medium enterprise minimum hardware requirements" on page 16.
  See "Large/very large enterprise minimum hardware requirements" on page 17.

If you install Oracle 11g on a dedicated server, that computer must meet the following minimum system requirements for Symantec Data Loss Prevention:

- One of the following operating systems:
  - Microsoft Windows Server 2003 (32-bit)
    (with Oracle Standard Edition only)
  - Microsoft Windows Server 2008 R2 (64-bit)
  - Microsoft Windows Server 2008 R2 SP1 (64-bit)
  - Red Hat Enterprise Linux 5.2 through 5.8 (32-bit)
    (with Oracle Standard Edition only)
  - Red Hat Enterprise Linux 5.2 through 5.8 (64-bit)
- 6 GB of RAM
- 6 GB of swap space (equal to RAM)
- 500 GB – 1 TB of disk space for the Enforce database

Note: Support for 32-bit platforms for Oracle will be discontinued in a future version of Symantec Data Loss Prevention. Symantec recommends that customers migrate to 64-bit systems as soon as possible.

On a Linux system, if the Oracle database is on the same computer as the Enforce Server, then the `/opt` file system must have at least 500 GB of free space for small or medium installations. 1 TB of free space is required for large or very large installations. If Oracle is installed on a different computer from the Enforce Server, then the `/opt` file system must have at least 10 GB of free space, and the `/boot` file system must have at least 100 MB of free space.

The exact amount of disk space that is required for the Enforce database depends on variables such as:

- The number of policies you plan to initially deploy
- The number of policies you plan to add over time
- The number and size of attachments you want to store (if you decide to store attachments with related incidents)
- The length of time you intend to store incidents

See the *Symantec Data Loss Prevention Administration Guide* for more information about developing policies.

See the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide* more Oracle installation information.

Browser requirements for accessing the Enforce Server administration console

Linux clients can access the Enforce Server administration console using Mozilla Firefox 3.x.

Windows clients can access the Enforce Server administration console using any of the following browsers:

- Microsoft Internet Explorer 8.x, 9.x
- Mozilla Firefox versions 8 through 12

Adobe Flash Player 10.1 is required to view the folder risk report for Network Discover (**Incidents > Discover > Folder Risk Report**).

See the *Symantec Data Loss Prevention Administration Guide* for information regarding browsers, languages, and character sets.

Requirements for using certificate authentication for single sign-on

Certificate authentication enables a user to automatically log on to the Enforce Server administration console using a client certificate that is generated by your public key infrastructure (PKI). To use certificate authentication, your PKI must deliver an X.509-compliant client certificate to the Tomcat container when a user access the Enforce Server administration console URL. The client certificate must contain a unique CN value that maps to an active user account in the Enforce Server configuration.

The client certificate must be delivered to the Enforce Server when a client's browser performs the SSL handshake with the Enforce Server administration console. For example, you might use a smart card reader and middleware with your browser to automatically present a certificate to the Enforce Server. Or, you might obtain an X.509 certificate from a certificate authority and upload the certificate to a browser that is configured to send the certificate to the Enforce Server.

Symantec Data Loss Prevention supports two mechanisms for checking whether a client certificate has been revoked: Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs). Symantec Data Loss Prevention can operate with an RFC 2560-compliant OCSP responder. If the OCSP responder cannot be reached, Symantec Data Loss Prevention will perform CRL validation using the method described in section 6.3 of RFC 3280. To use CRL validation, each client certificate must include the HTTP URL of a CRL distribution point (CRLDP). Symantec Data Loss Prevention extracts the HTTP URL from the CRL distribution point extension to the X.509 certificate. Note, however, that Symantec Data Loss Prevention cannot use LDAP URLs that are embedded in the CRL distribution point extension.

For more information about configuring certificate authentication and certificate revocation checks, see the *Symantec Data Loss Prevention System Administration Guide*.

Virtual server and virtual workstation support

Symantec supports running certain Symantec Data Loss Prevention components on the following virtualization products:

Table 1-9

VMWare version	Enforce Server	Endpoint Prevent Server	Network Discover Server	Network Prevent for Email Server	Network and Mobile Prevent for Web Server	Classification Server (Microsoft Windows only)
VMware ESX version 3.5 (32-bit or 64-bit hardware)	Yes	No	Yes	Yes	Yes	Yes
VMware ESX version 4.0 (64-bit hardware)	Yes	Yes*	Yes	Yes	Yes	Yes
VMware ESX and ESXi version 4.1 (64-bit hardware)	Yes	Yes*	Yes	Yes	Yes	Yes

Note: *Endpoint Prevent servers are supported only for configurations that do not exceed the recommended number of connected agents.

For more information, see article number 54539, "Symantec™ Data Loss Prevention Endpoint Server Scalability on VMware," at the Symantec Data Loss Prevention Knowledgebase, at https://kb-vontu.altiris.com/article.asp?article=54539&p=4.

Symantec also supports running the Symantec DLP Agent software on virtual workstations using VMware Workstation 6.5.x. This is in addition to the support for running the DLP Agent software on Citrix virtual desktops and virtual applications.

See "Virtual desktop and virtual application support with Endpoint Prevent" on page 32.

Symantec does not support running the Oracle database server on virtual hardware. If you deploy the Enforce Server to a virtual machine, you must install the Oracle database using physical server hardware (a three-tier deployment).

Symantec does not support running the Network Monitor or Mobile Prevent for Web detection servers on virtual machines.

At a minimum, ensure that each virtual server environment matches the system requirements for servers described in this document.

See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 15.

Note that a variety of factors influence performance of virtual machine configurations, including the number of CPUs, the amount of dedicated RAM, and the resource reservations for CPU cycles and RAM. The virtualization overhead and guest operating system overhead can lead to a performance degradation in

throughput for large datasets compared to a system running on physical hardware. Use your own test results as a basis for sizing deployments to virtual machines.

See the *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines* for additional information about running Network Prevent servers on virtual machines.

Virtual desktop and virtual application support with Endpoint Prevent

Citrix XenDesktop and Citrix XenApp provide virtual Windows desktops and Windows applications to clients of the Citrix servers. Symantec supports deploying the Symantec DLP Agent software directly on Citrix XenApp/Application servers or Citrix XenDesktop virtual machines to prevent clients from extracting confidential data from Citrix published applications or desktops to the client computer. Symantec Data Loss Prevention provides this functionality by monitoring volumes, print/fax requests, clipboards, and network activity on the Citrix server to detect when confidential data would be sent to a client computer. A Symantec DLP Agent does not need to be installed on each individual Citrix client to support this functionality. A single Symantec DLP Agent monitors all of the Citrix clients. All Citrix clients that are protected by the agent monitor need to have a valid Endpoint Prevent license. The license is required whether a Symantec DLP Agent is installed on the client or not.

Note: All incidents that are generated on Citrix drives by the Symantec DLP Agent software appear as **Removable Storage Device** incidents. In the Enforce Server administration console, you cannot deselect the **Removable Storage** event for Citrix drives because this event is always monitored by agents that are deployed to Citrix servers.

The following Citrix products are supported, with the indicated limitations:

Table 1-10 Citrix virtualization support and limitations

Supported Citrix products	Endpoint Prevent use case	Limitations
■ Citrix XenApp 4.5 on Windows Server 2003 (32-bit) Enterprise Edition SP2 ■ Citrix XenApp 6 on Windows 2008 Enterprise Edition R2 (64-bit) ■ Citrix XenApp 6.5 on Windows 2008 Enterprise Edition R2 (64-bit)	Prevents users from extracting confidential data from XenApp published applications to a client computer.	Performance and deployment: ■ You must install the Symantec DLP Agent software on each XenApp server host, and on any individual application servers that publish applications through XenApp. ■ All detection on Citrix XenApp is performed in a single thread (all user activities are analyzed sequentially). ■ Symantec tests indicate that the Symantec DLP Agent software can support a maximum of 40 simultaneous clients per Citrix server. However, detection performance varies depending on the server hardware, the type of applications that are used, and the activities that Citrix clients perform. You must verify the Symantec DLP Agent performance characteristics for your environment. ■ The Symantec DLP Agent software should connect to an Endpoint Prevent server that is reserved for Citrix agents. Using the same Endpoint Prevent server for non-Citrix agents limits the functionality of those agents, because you must disable Local Drive and CD/DVD monitoring for the server as a whole. See "Detection server restriction for Symantec DLP Agents on Citrix XenApp" on page 34. ■ When you use the Enforce Server administration console to configure endpoint events to monitor, you must deselect CD/DVD and Local Drive events for XenApp agents. These items are present on the server configuration page, but they are not supported for Citrix XenApp. Endpoint Prevent features: ■ Symantec DLP Agents that are deployed to Citrix XenApp servers cannot detect confidential data in an HTTP/S attachment if the attachment is from an Endpoint-published drive. Detection is performed if the attachment is from a server local drive or from a file server that is accessible to the Citrix Published App. ■ If XenApp streams an application directly to an endpoint computer, the Symantec DLP Agent that is deployed to XenApp server cannot monitor the streamed application. ■ FTP events are not supported. ■ Printer/Fax events for files on endpoint-published drives are not monitored for Adobe Acrobat Reader. ■ Instant messenger events (MSN IM, Yahoo IM, and AIM) have not been tested and are not supported. ■ IP addresses in Data Loss Prevention incident snapshots contain the IP address of the XenApp server, and not a Citrix client. ■ If the Symantec DLP Agent software blocks an attempted copy to a client drive, it does not provide an option to restore or recover the file at a later time.

Table 1-10 Citrix virtualization support and limitations *(continued)*

Supported Citrix products	Endpoint Prevent use case	Limitations
■ Citrix XenDesktop 3.0 with Windows XP SP3 or Windows 7 (32-bit or 64-bit) ■ Citrix XenDesktop 4 on Windows XP SP3, Windows 7 (32-bit or 64-bit) ■ Citrix XenDesktop 5.0 on Windows XP SP3, Windows 7 SP1 (32-bit or 64-bit)	Prevents users from extracting confidential data from a virtualized Windows desktop to the local client computer.	Performance and deployment: ■ You must install the Symantec DLP Agent software on each virtual machine on the XenDesktop server. ■ The Symantec DLP Agent software can connect either to a dedicated Endpoint Prevent server or to an Endpoint Prevent server that is shared with non-Citrix agents. You cannot connect to an Endpoint Prevent server that is reserved for Citrix XenApp. Note that if you use the same server for both Citrix and non-Citrix agents, you cannot configure events independently for each environment. Endpoint Prevent features: ■ Symantec DLP Agents that are deployed to Citrix XenDesktop VMs cannot detect confidential data in an HTTP/S attachment if the attachment is from an Endpoint-published drive. Detection is performed if the attachment is from a server local drive or from a file server that is accessible to the Citrix Published Desktop. ■ FTP events are not supported. ■ Printer/Fax events for files on endpoint-published drives are not monitored for Adobe Acrobat Reader. ■ Instant messenger events (MSN IM, Yahoo IM, and AIM) have not been tested and are not supported. ■ IP addresses in Data Loss Prevention incident snapshots contain the IP address of the XenDesktop virtual machine, and not a Citrix client. ■ If the Symantec DLP Agent software blocks an attempted copy to a client drive, it does not provide an option to restore or recover the file at a later time.

Detection server restriction for Symantec DLP Agents on Citrix XenApp

Symantec does not recommend using a single Endpoint Prevent detection server with both physical endpoint computers and Citrix XenApp servers. When you use the Enforce Server administration console to configure endpoint events to monitor, you must deselect CD/DVD and Local Drive events for Citrix XenApp agents. (These items are present on the server configuration page, but they are not supported for Citrix XenApp.) Using the same Endpoint Prevent Server for non-Citrix agents limits the functionality of those agents, because you must disable Local Drive and CD/DVD events for the server as a whole.

To support Symantec DLP Agent software on both Citrix XenApp servers and physical endpoint computers, Symantec recommends that you deploy two Endpoint

Prevent detection servers and ensure that each server is reserved for either Citrix XenApp agents or physical endpoint agent installations.

Third-party software requirements and recommendations

Symantec Data Loss Prevention requires certain third-party software. Other third-party software is recommended. See:

- Table 1-11 for required software
- Table 1-12 for required Linux RPMs
- Table 1-13 for recommended software

Table 1-11 Required third-party software

Software	Required for	Description
Adobe Reader	All systems	Adobe Reader is required for reading the Symantec Data Loss Prevention documentation. Download from Adobe.
Apache Tomcat version 7.0.23.0	Enforce Server	Required to support the reporting system. The correct version of Tomcat is automatically installed on the Enforce Server by the Symantec DLP Installation Wizard and does not need to be obtained or installed separately.
Java Runtime Environment (JRE) 1.6.0_31	All servers	The Symantec DLP Installation Wizard automatically installs the correct JRE version.
Napatech driver version 4.22	Napatech NT4E-STD high-speed packet capture card	Provides high-speed montitoring.
WinPcap 4.1.1 or later	Required for Windows-based Network Monitor Server. Recommended for all Windows-based detection servers.	Windows packet capture library. Download from winpcap.org.

Table 1-11 Required third-party software *(continued)*

Software	Required for	Description
Endace card driver 3.2.1, .3.2.2, 3.3.1 or 3.4.2	Detection servers equipped with an Endace network measurement card.	Download from Endace. See "Small/medium enterprise minimum hardware requirements" on page 16.
VMware ESX version 3.5, 4.0, or 4..1, or ESXi version 4.1.	Required to run supported components in a virtualized environment. See "Virtual server and virtual workstation support" on page 30.	Virtualization software. Download from VMware.
Microsoft Active Directory 2003 or 2008 R2	Required versions for connecting to Active Directory.	Provides directory services for Windows domain networks.

In addition to the Linux Minimal Installation, Linux-based Symantec Data Loss Prevention servers require the Red Hat Package Managers (RPM) listed in Table 1-12.

Table 1-12 Required Linux RPMs

Linux-based servers	Required RPMs

Enforce Server
Oracle server
	`apr`
	`apr-util`
	`binutils`
	`compat-libstdc++-296`
	`compat-libstdc++-33`
	`expat`
	`Xorg-x11*`
	*Required only for graphical installation. Console-mode installation does not require an X server.

Network Monitor Server	`apr`
	`apr-util`
	`compat-libstdc++-296`
	`compat-libstdc++-33`
	`expat`
	`Xorg-X11*`
	*Required only for graphical installation. Console-mode installation does not require an X server.

Note: SeLinux must be disabled on all Linux-based servers.

Symantec recommends the third-party software listed in Table 1-13 for help with configuring and troubleshooting your Symantec Data Loss Prevention deployment.

Table 1-13 Recommended third-party software

Software	Location	Description
Wireshark	Any server computer	Use Wireshark (formerly Ethereal) to verify that the detection server NIC receives the correct traffic from the SPAN port or tap. You can also use Wireshark to diagnose network problems between other servers. Download the latest version from Wireshark.
dagsnap	Network Monitor Server computers that use Endace cards	Use in combination with Wireshark to verify that the detection server Endace NIC receives the correct traffic from the SPAN port or tap. Dagsnap is included with Endace cards, and is not required with non-Endace cards.
Sysinternals Suite	Any Windows server computer	Troubleshooting utilities. Recommended for diagnosing problems on Windows server computers. Download the latest version from Microsoft.
LDAP browser	Enforce Server	An LDAP browser is recommended for configuring or troubleshooting Active Directory or LDAP.

Chapter 2

Product compatibility

This chapter includes the following topics:

Environment compatibility and requirements for Network Prevent for Email

The Network Prevent for Email Server is compatible with a wide range of enterprise-grade third-party SMTP-compliant MTAs and hosted email services. Consult your MTA vendor or hosted email service for specific support questions.

Network Prevent for Email Server can integrate with an MTA or hosted email service that meets the following requirements:

- The MTA or hosted email service must be capable of strict SMTP compliance. It must be able to send and receive mail using only the following command verbs: HELO (or EHLO), RCPT TO, MAIL FROM, QUIT, NOOP, and DATA.

- When running the Network Prevent for Email Server in reflecting mode, the upstream MTA must be able to route messages to the Network Prevent for Email Server once and only once for each message.

In practice, these requirements mean that you can use an SMTP-compliant MTA that can route outbound messages from your internal mail infrastructure to the Network Prevent for Email Server. For reflecting mode compatibility, the MTA must also be able to route messages that are returned from the Network Prevent for Email Server out to their intended recipients.

Network Prevent for Email Server attempts to initiate a TLS connection with a downstream MTA only when the upstream MTA issues the STARTTLS command. The TLS connection succeeds only if the downstream MTA or hosted email service supports TLS and can authenticate itself to the Network Prevent for Email Server. Successful authentication requires that the appropriate keys and X509 certificates are available for each mail server in the proxied message chain.

See the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent for Email* for information about configuring TLS support for Network Prevent for Email servers operating in forwarding mode or reflecting mode.

Proxy server compatibility with Network Prevent for Web

Network Prevent for Web Servers used the ICAP protocol and can operate with the following proxies:

Table 2-1 Network Prevent for Web supported proxy servers

Proxy	Supported protocols	Configuration information
Blue Coat ProxySG version 4.2.1, 5.2.4.8, 5.5.2.1, and 5.5.3.1 for Network Prevent for Web Blue Coat ProxySG version 5.5.3.1 for Mobile Prevent, or for Mobile Prevent deployed with Network Prevent for Web	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Blue Coat product documentation
Cisco IronPort S-Series version 6.0, 7.1.2	HTTP, HTTPS, FTP over HTTP	Cisco IronPort product documentation

Table 2-1 Network Prevent for Web supported proxy servers *(continued)*

Proxy	Supported protocols	Configuration information
Microsoft ISA 2004, 2006 Standard and Enterprise editions	HTTP, limited FTP over HTTP	See the *Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server*
Microsoft TMG 2010 (without service pack, or with SP1 or SP2) on Microsoft Windows 2008 R2 SP1 Enterprise or Standard Edition	HTTP, HTTPS, limited FTP over HTTP/S	See the *Symantec Data Loss Prevention Integration Guide for Microsoft Threat Management Gateway*
Secure Computing Secure Web (Webwasher) versions 6.8.x and 6.9.1	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Secure Web documentation (particularly the chapter that describes setting up Secure Web with a DLP Solution)
McAfee Web Gateway versions 6.9 and 7.2	HTTP, HTTPS, FTP over HTTP, or FTP proxy	McAfee product documentation. Supported in Symantec Data Loss Prevention version 11.6.
Squid Web Proxy version 3.0 and 3.1.11 Stable 18 (Linux only)	HTTP	See the *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy*
Symantec Web Gateway versions 5.0 and 5.0.2.8	HTTP, HTTPS	See the *Symantec Web Gateway 5.0 Implementation Guide*

Table 2-1 Network Prevent for Web supported proxy servers *(continued)*

Proxy	Supported protocols	Configuration information
Websense Appliance V5000 and V10000, with Websense Web Security version 7.6.0 (11.1.1 and later)	HTTP, HTTPS	Does not support redaction. Only supports "Block HTTP/HTTPS". `RESPMOD` is not supported. Websense blocks the traffic only when the size of the Symantec Data Loss Prevention rejection message (in the response rule) is larger than 512 bytes. If the rejection messages is less than 512 bytes, an incident is generated but the network traffic is not blocked.

High-speed packet capture cards

This topic describes the high-speed packed capture cards that are supported for Network Prevent.

Table 2-2 Supported high-speed packet capture cards

Card	Version	Driver version
Endace	■ EDM01-01v7_DAG_3.7 ■ EDM01-01v7_DAG_4.3GE ■ DAG_4.5 G2/G4 (PCI-X) ■ DAG_7.5 G2/G4 (PCI-E) **Note:** Endace cards for use with Data Loss Prevention are supported on Linux 32- and 64-bit systems; for Windows, Endace cards are supported for use with Data Loss Prevention on 32-bit systems only.	3.2.1, .3.2.2, 3.3.1 or 3.4.2
Napatech (64-bit hardware only)	NT4E-STD	4.22

Data Insight compatibility with Symantec Data Loss Prevention version 11.x

Symantec Data Insight is a separately licensed option to Symantec Data Loss Prevention that helps organizations solve the problem of identifying data owners and responsible parties for information due to incomplete or inaccurate metadata or tracking information. Symantec Data Insight provides a connection from the Enforce Server to a Symantec Data Insight Management Server.

With Data Insight Version 2.5, Symantec Data Loss Prevention version 11.6 does not pull SharePoint activities (including file owner, access history, and folder risk score) in to the incident data. See the *Symantec Data Loss Prevention Data Insight Implementation Guide* that is included with Symantec Data Loss Prevention.

Table 2-3 Supported versions of Symantec Data Insight for Symantec Data Loss Prevention version 11.x

Symantec Data Insight Version	DLP version 11.0	DLP version 11.1	DLP version 11.5	DLP version 11.6
2.0	Yes	Yes	Yes	Yes
2.5	No	Yes	Yes	Yes. No SharePoint activities included in incident data.
3.0	No	Yes	Yes	Yes
3.0 RP1	No	Yes	Yes	Yes
3.0 RP2	No	Yes	Yes	Yes
3.0.1	No	Yes	Yes	Yes

Symantec Veritas Cluster Server compatibility

Symantec Veritas Cluster Server (VCS) is a high-availability solution that provides failover capabilities for the Symantec Data Loss Prevention Enforce Server and Oracle database hosts.

Table 2-4 describes Data Loss Prevention and VCS compatibility according to operating system platform.

Table 2-4 Data Loss Prevention and VCS compatibility

Operating system	Symantec Data Loss Prevention version	VCS version
Microsoft Windows 64-bit	11.1 and later	5.1 SP2
Microsoft Windows 64-bit	11.5 and later	6.0
Linux 64-bit	11.5 and later	5.1 SP1, 6.0

Symantec / Symantec Data Loss Prevention integrations

This section describes compatibility of various integrations of Symantec Data Loss Prevention with other Symantec products.

Table 2-5 Symantec product compatibility with Symantec Data Loss Prevention

Symantec product	Version	Note	DLP version 11.0	DLP version 11.1	DLP version 11.5	DLP version 11.6
Symantec PGP Universal Gateway Email	2.63		Yes	Yes	Yes	Yes
Symantec Messaging Gateway (SMG)	7.5		Yes	Yes	Yes	Yes
	8.0		Yes	Yes	Yes	Yes
	10.0		No	No	Yes	Yes
Altiris NS	7.0		Yes	Yes	Yes	Yes
Symantec Web Gateway (SWG)	5.0		No	No	Yes	Yes
	5.0, 5.0.2.8		No	No	Yes	Yes

Table 2-5 Symantec product compatibility with Symantec Data Loss Prevention *(continued)*

Symantec product	Version	Note	DLP version 11.0	DLP version 11.1	DLP version 11.5	DLP version 11.6
Symantec Enterprise Vault	10.0		Yes	Yes	Yes	No
	10.0.1		No	No	Yes	Yes
Symantec Management Platform (SMP)	7.0 SP2 or later		No	Yes	Yes	Yes
	7.0 SP3 or later for DLP Agent on Microsoft Windows 7		No	Yes	Yes	Yes
Symantec Data Insight	2.0	See "Data Insight compatibility with Symantec Data Loss Prevention version 11.x" on page 43.	Yes	Yes	Yes	Yes
	2.5		No	Yes	Yes	Yes
	3.0		No	Yes	Yes	Yes
	3.0 RP1		No	Yes	Yes	Yes
	3.0 RP2		No	Yes	Yes	Yes
	3.0.1		No	Yes	Yes	Yes
Symantec Mobile Management (SMM)	7.1 SPI		No	No	Yes	Yes
	7.2		No	No	Yes	Yes

Table 2-5 Symantec product compatibility with Symantec Data Loss Prevention *(continued)*

Symantec product	Version	Note	DLP version 11.0	DLP version 11.1	DLP version 11.5	DLP version 11.6
Symantec Veritas Cluster Server	For Windows 64-bit: 5.1 SP2	High-availability solution for the Enforce Server and Oracle database. See "Symantec Veritas Cluster Server compatibility" on page 43.	No	Yes	Yes	Yes
	For Windows 64-bit: 6.0		No	No	Yes	Yes
	For Linux 64-bit: 5.1 SP1		No	No	Yes	Yes
	For Linux 64-bit: 6.0		No	No	Yes	Yes

Network Discover compatibility

Network Discover locates exposed confidential data by scanning a broad range of enterprise data repositories such as: file servers, databases, Microsoft SharePoint, Lotus Notes, Documentum, Livelink, Microsoft Exchange, and Web servers.

See "Supported file system targets" on page 47.

See "Supported Lotus Notes targets" on page 47.

See "Supported SQL database targets" on page 48.

See "Supported SharePoint server targets" on page 48.

See "Supported Exchange Server Web Store connector targets" on page 49.

See "Supported Exchange Server Web Services connector targets" on page 49.

See "Supported file system scanner targets" on page 50.

See "Supported Exchange scanner targets" on page 50.

See "Supported SharePoint scanner targets" on page 51.

See "Supported Documentum (scanner) targets" on page 52.

See "Supported Livelink scanner targets" on page 52.

See "Supported Web server (scanner) targets" on page 52.

Supported file system targets

The File System target supports scanning of the following network file systems:

Supported file servers:

- CIFS Servers only

Supported file shares:

- CIFS on Windows
- NFS on Linux
- DFS scanning on Windows 2003 and 2008.

Note: DFS is not supported with Network Protect.

In addition, the File Systems 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 on that system.
- File systems on UNIX systems, even if they are not exposed as CIFS or NFS shares.
  Use the SFTP protocol to provide a method similar to the scans of file shares. You can also scan the local file system on a Linux Network Discover Server by listing the path name in the content root. For example, you can enter `/home/myfiles`.

Supported Lotus Notes targets

The Lotus Notes target supports scanning of the following versions:

- Lotus Notes 6.5
- Lotus Notes 7.0
- Lotus Notes 8.0

- Lotus Notes 8.5.1

On Network Discover 32-bit servers, the native configuration is recommended, and a 32-bit Lotus Notes client must be installed on the Network Discover Server.

64-bit Windows Servers support the DIIOP configuration option. 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 in both DIIOP and native configurations.

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

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.

Supported SharePoint server targets

The following SharePoint server targets are supported:

- Microsoft Office SharePoint Server 2003 on Windows Server 2003, 32-bit SharePoint 2003 is supported only with the SharePoint scanner.
- Microsoft Office SharePoint Server 2007, on Windows Server 2003, 32-bit
- Microsoft Office SharePoint Server 2007, on Windows Server 2003, 32-bit or 64-bit, or Windows Server 2008 R1, 32-bit or 64-bit
- Microsoft Office SharePoint Server 2010, on Windows Server 2008 R2, 64-bit

See "Supported SharePoint scanner targets" on page 51.

Supported Exchange Server Web Store connector targets

The Exchange Web Store connector supports the following Exchange Server targets:

- Microsoft Exchange Server 2003
- Microsoft Exchange Server 2007
  For Exchange 2007 SP2 servers, you can either use the Exchange Web Store connector or Exchange Web Services connector.

To use the Exchange Web Store connector, Outlook Web Access must be configured, and WebDAV must be enabled.

The Exchange scan includes email message text and email file attachments from the user's mailbox.

You can scan the data objects that are stored within Public Folders, such as:

- Email messages
- Message attachments
- Microsoft Word documents
- Excel spreadsheets

The Exchange scan does not target mail stored in Personal Folders (`.pst` files) or offline folders (`.ost` files) that are not on the Exchange server. To scan `.pst` files on a file share, use the shared file system target.

Supported Exchange Server Web Services connector targets

The Exchange Web Services connector supports the following Exchange Server targets:

- Microsoft Exchange Server 2007 SP2 or later
  For Exchange 2007 SP2 servers, you can either use the Exchange Web Services connector or the Exchange Web Store connector.
- Microsoft Exchange Server 2010

To use the Exchange Web Services connector, Exchange Web Services and the Autodiscover Service must be enabled on your Exchange server and are accessible to the Network Discover server.

You can scan the data objects that are stored within Public Folders, such as:

- Email messages
- Message attachments
- Microsoft Word documents

- Excel spreadsheets

The Exchange scan also targets mail stored in Exchange 2010 Personal Archives.

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 U5

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:

- `xlC.aix50.rte` (v8.0.0.0+)
- `xlC.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.

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.

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.

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_11.6.exe`
  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, 32-bit or 64-bit, or Windows 2008 R1, 32-bit or 64-bit.

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_11.6.exe`

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

Make sure the correct SharePoint scanner is installed for your version of SharePoint.

Supported Documentum (scanner) targets

The Documentum scanner supports scanning a Documentum Content Server 5.3.x repository.

Supported Livelink scanner targets

The Livelink scanner supports scanning of the following targets:

- Livelink Server 9.x

Supported Web server (scanner) targets

The Web server scanner supports scanning of a static HTTP Web site.

About Endpoint Data Loss Prevention compatibility

Endpoint Data Loss Prevention is compatible with different operating systems and software applications.

See "Endpoint Data Loss Prevention supported operating systems" on page 52.

See "Endpoint Prevent supported applications" on page 53.

Endpoint Data Loss Prevention supported operating systems

Endpoint Data Loss Prevention can operate on Endpoint systems that use the following operating systems:

Table 2-6 Endpoint Data Loss Prevention supported operating systems

Operating system	Version	Symantec Data Loss Prevention			
		Version 10.0	Version 10.5	Version 11.0	Versions 11.1x, 11.5, and 11.6
Windows XP Professional (32-bit)	SP2	Yes	Yes	Yes	Yes
	SP3	Yes	Yes	Yes	Yes
Windows Server 2003 (32-bit)	SP1	Yes	No	No	No
	SP2	Yes	Yes	Yes	Yes
	R2	Yes	Yes	Yes	Yes
Windows Vista Enterprise (32-bit)	unpatched	Yes	No	No	No
	SP1	Yes	Yes	Yes	Yes
	SP2	No	No	No	Yes
Windows 7 Enterprise, Professional, Ultimate (32-bit)	SP1	Yes (Windows 7 only, not SP1)	Yes (Windows 7 only, not SP1)	Yes (Windows 7 only, not SP1)	Yes (11.1.1 and later only)
Windows 7 Enterprise, Professional, Ultimate (64-bit)	SP1	No	Yes (Windows 7 only, not SP1)	Yes (Windows 7 only, not SP1)	Yes (11.1.1 and later only)
Microsoft Windows 2008 Enterprise or Standard R2 (64-bit)	R2	No	No	No	Yes

Endpoint Prevent supported applications

This following table describes individual applications that can be monitored using Endpoint Prevent.

Endpoint Prevent enables you to add monitoring support for other third-party applications not listed in this table. Examples of third-party applications include

Skype, Thunderbird, and Google Chrome. Any application that is not specifically monitored by Symantec Data Loss Prevention must be configured for application monitoring before Symantec Data Loss Prevention can detect content with those applications. Always test individual third-party applications before you enable monitoring on a large number of endpoints. Individual applications may need additional filtering settings to maintain acceptable performance. See the *Symantec Data Loss Prevention System Administration Guide* for more information about configuring and using application monitoring.

Table 2-7 Applications supported by Endpoint Prevent

Feature	Software	Version	Symantec Data Loss Prevention			
			Version 9.x	Version 10.0	Version 10.5	Versions 11.x
HTTP	All browsers	All	Yes	Yes	Yes	Yes
Secure HTTP (HTTPS)	Internet Explorer	6.0	Yes	Yes	Yes	Yes
		7.0	Yes	Yes	Yes	Yes
		8.0	Yes (9.0.1 only)	Yes	Yes	Yes
		9.0	No	No	No	Yes (11.1.1 and later)
	Firefox	2.0	Yes	Yes	Yes	Yes
		3.0	Yes	Yes	Yes	Yes
		3.5	No	Yes	Yes	Yes
		3.6	No	No	Yes	Yes
		4.0	No	No	No	Yes (11.1.1 and later)
Instant messaging	Yahoo Messenger	7.5	Yes	Yes	Yes	Yes
		8.0	Yes	Yes	Yes	Yes
		8.1	Yes	Yes	Yes	Yes
		9.0	No	Yes	Yes	Yes
		10.0	No	No	Yes	Yes

Table 2-7 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention			
			Version 9.x	Version 10.0	Version 10.5	Versions 11.x
	MSN Messenger	8.1	Yes	Yes	Yes	Yes
		9.0 (14)	No	Yes	Yes	Yes
	AIM	5.9	Yes	Yes	Yes	Yes
		6.0	Yes	Yes	Yes	Yes
		6.1	Yes	Yes	Yes	Yes
		6.5	No	Yes	Yes	Yes
		6.8	No	Yes	Yes	Yes
		6.9	No	Yes	Yes	Yes
	AIM Pro	1.4	*Yes	Yes	Yes	Yes
		1.5	*Yes	Yes	Yes	Yes
Email	Outlook	2002	Yes	Yes	Yes	Yes
		2003	Yes	Yes	Yes	Yes
		2007	Yes	Yes	Yes	Yes
		2010 (32-bit and 64-bit)	No	No	No	Yes
	Eudora		No	No	No	No
	Thunderbird		No	No	No	No
	Lotus Notes	6.5	No	No	Yes	Yes
		7.0	Yes	Yes	Yes	Yes
		8.0	Yes	Yes	Yes	Yes
		8.5	No	Yes	Yes	Yes
		8.5.1				Yes (11.1.1 and later)
		8.5.3				Yes (11.1.1 and later)

Table 2-7 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention			
			Version 9.x	Version 10.0	Version 10.5	Versions 11.x
FTP			Yes	Yes	Yes	Yes
CD/DVD	BsClip		Yes	Yes	Yes	Yes
	Bs Recorder Gold		Yes	Yes	Yes	Yes
	BurnAware		Yes	Yes	Yes	Yes
	Cheetah Burner		Yes	Yes	Yes	Yes
	Command Burner		Yes	Yes	Yes	Yes
	CopyToDVD		Yes	Yes	Yes	Yes
	Creator10		Yes	Yes	Yes	Yes
	Deep Burner (32-bit Windows XP)		Yes	Yes	Yes	Yes
	GEAR for Windows		Yes	Yes	Yes	Yes
	mkisofs		Yes	Yes	Yes	Yes
	Nero		Yes	Yes	Yes	Yes
	NeroStartSmart		Yes	Yes	Yes	Yes
	Roxio		Yes	Yes	Yes	Yes
	Roxio RecordNow		Yes	Yes	Yes	Yes
	Roxio5		Yes	Yes	Yes	Yes
	Roxio Mediahub		Yes	Yes	Yes	Yes
	Silent Night Micro Burner		Yes	Yes	Yes	Yes
	Star Burn		Yes	Yes	Yes	Yes

Table 2-7 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention			
			Version 9.x	Version 10.0	Version 10.5	Versions 11.x
	Windows native CD/DVD writer					Yes

*Note that Endpoint Prevent 9.x does not support AIM Pro 1.4 and 1.5 when they are used in encrypted mode.

Mobile Prevent compatibility

Symantec Data Loss Prevention Mobile Prevent monitors email, Web, and application communications from mobile devices to prevent sensitive information from leaving your organization. Configuring and deploying a VPN profile for the mobile devices routes the network communication from the mobile device; then, through a VPN and into your corporate network proxy server.

Compatibility and configuration information is available to assist in deploying Symantec Data Loss Prevention Mobile Prevent. See "Symantec Data Loss Prevention for Mobile compatibility" on page 73.

Chapter 3

Symantec DLP Agent Compatibility With Other Applications

This chapter includes the following topics:

About using Symantec DLP Agent with other applications

The Symantec DLP Agent is installed on endpoint computers, and it interoperates with many other applications.

See "Operating system requirements for endpoint systems" on page 21.

The agent generally works seamlessly with other applications. However, in some cases you need to configure an application to enable the agent to function properly. The most common adjustments and configurations are required for antivirus and firewall applications, which fall into two these categories:

- Server-side
  See "Symantec DLP Agent and server-side application configuration" on page 60.
- Client-side

See "Symantec DLP Agent and client-side application configuration" on page 67.

The following sections provide instructions for white-listing the Symantec DLP Agent with selected third-party applications. Other applications that are not listed in these sections may also require changes to permit the Symantec DLP Agent to function. In these cases, refer to your third-party application documentation and follow the instructions to white-list individual applications and processes.

Symantec DLP Agent and server-side application configuration

You must make a few configuration changes to a number of server products. If you do not make these changes, the Symantec DLP Agent cannot function properly. The server products that are affected are:

- Cisco CSA - Management Center
  See "Configuring Cisco CSA Management Center to work with Symantec DLP Agent (server-side)" on page 60.
- McAfee ePolicy Orchestrator 4.0
  See "Configuring McAfee ePolicy Orchestrator to work with Symantec DLP Agent (server-side)" on page 61.
- McAfee Total Protection Service
  See "Configuring McAfee Total Protection Service to work with Symantec DLP Agent (server-side)" on page 62.
- Sophos Enterprise Console
  See "About Sophos Enterprise Console and Symantec DLP Agent" on page 63.
- Symantec Critical System Protection
  See "Configuring Symantec Critical System Protection to work with Symantec DLP Agent (server-side)" on page 65.

Configuring Cisco CSA Management Center to work with Symantec DLP Agent (server-side)

The Symantec DLP Agent should be defined as a white-listed application in order for the CSA agent to ignore it.

To modify Cisco CSA Management Center

1. From the main menu bar, go to **Configuration > Application > Application Classes**.
2. Select **Administrator Defined - White List Application**.
3. In the **Add process to application** class, double-click the **$Administrator defined - White List files [V6.0 r205]** variable.
4. In the Directory Matching section, enter **@program_files**\\Manufacturer\\Endpoint Agent*** where @program_files is a variable which would be expanded to the program files path.

   This path should be the path where the Symantec DLP Agent is installed.
5. In the Files Matching section, enter **edpa.exe** and **wdp.exe**.
6. Click **Save**.
7. Click **Generate Rules > Generate**.

   This command pushes the configuration to the CSA Agent.

Note: This configuration enables the Symantec DLP Agent to operate with the CSA agent. However, Clipboard and Print/Fax functionality are still disabled because of hooking failures within the agent. All other monitoring functions operate correctly.

Configuring McAfee ePolicy Orchestrator to work with Symantec DLP Agent (server-side)

Symantec DLP Agent installation is blocked in McAfee if access protection is enabled for endpoint systems. To install or uninstall Symantec DLP Agent when Maximum Protection rules are enabled, first disable Access Protection on ePolicy. Perform the installation or uninstallation, and then turn on Access Protection when you are finished.

To disable Access Protection

1. On the Main page of the ePolicy Orchestrator server, open the **Systems** menu.
2. Click the **Access Protection** tab.

3 Under the section Access protection settings uncheck **Enable access protection**.

4 Click **Save**.

The Access protection is disabled on all the clients the next time the policy is rolled out to the clients.

To configure McAfee ePolicy Orchestrator 4.0

1 Click the **Policy Catalog** tab.

2 Select the product **Virusscan Enterprise x.x.x** where x is the version number of the product.

3 Select the category as **Access Protection policies**.

4 All existing policies are listed. Edit the policy you want by clicking the **Edit** icon next to the policy.

5 On the Edit page, select the category settings for **Domain / Workstation** and enable authorization.

6 Click the **Access Protection** tab and enable access protection.

Configuring McAfee Total Protection Service to work with Symantec DLP Agent (server-side)

By default, McAfee Total Protection Service blocks the Symantec DLP Agent (`edpa.exe`) from communicating with the Endpoint Server. To avoid this problem, create a custom server policy that allows `edpa.exe` to communicate with the Endpoint Server. Then use this policy when installing McAfee Total Protection Service onto client computers.

If you already installed McAfee Total Protection onto computers without using a custom policy, the software blocks `edpa.exe`. In this case, configure the McAfee Total Protection Firewall on the client computer to allow full access for `edpa.exe`.

See "Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side)" on page 70.

To create a custom server policy for edpa.exe access

1 Log on to the McAfee security center from a computer where you already installed the Symantec DLP Agent. The security center is available at `http://www.mcafeeasap.com/asp_securitycenter/default.asp`.

2 Select **Groups + Policies > Add Policy**.

3 Type a name for the new policy in the **Policy name** field.

4 Select the **Desktop Firewall** tab.

5 Select the **Administrator configures firewall** option.

6 In the **Allowed Internet Applications** list, find the `edpa.exe` application. Click the **Allow** button next to the `edpa.exe` application to allow full access.

7 Click **Save** to save the new policy.

8 In the **Group** list, select the **Assign Policy** link next to the **Default Group** entry.

9 Select the name of the new policy you created from the **Policy used by group menu**.

10 Click **Save** to save changes to the default group.

When you perform new installations of McAfee Total Protection Service, the custom policy is applied and client computers allow full access for the `edpa.exe` application.

About Sophos Enterprise Console and Symantec DLP Agent

You must authorize the files and the drivers that are related to Symantec DLP Agent through this console. This task is achieved by modifying the policies for:

- Sophos Anti-virus
  See "Configuring Sophos Anti-virus to work with Symantec DLP Agent (server-side)" on page 63.
- Sophos Firewall systems
  See "Configuring Sophos Firewall to work with Symantec DLP Agent (server-side)" on page 64.
- Sophos Application Control
  See "Configuring Sophos Application Control to work with Symantec DLP Agent (server-side)" on page 64.

Configuring Sophos Anti-virus to work with Symantec DLP Agent (server-side)

You must configure Sophos Anti-virus to work with the Symantec DLP Agent.

To configure Sophos Anti-virus

1 Expand the Antivirus and HIPS under Policies section on the console home page.

2 Select the policy that you want to authorize.

3 On the **AV and HIPS policy** tab, select **HIPS runtime behavior.**

4 In the **Authorization Manager** window, add **edpa.exe**, **wdp.exe**, **vfsmd.sys**, and **vrtam.sys** to the authorized files list. This procedure should be done for both **Suspicious Files** and **Suspicious Behavior** sections.

5 Click **OK**.

Configuring Sophos Firewall to work with Symantec DLP Agent (server-side)

You must configure Sophos Firewall to work with the Symantec DLP Agent.

To configure Sophos Firewall

1 On the console home page, click the **Firewall** option under the Policies section.

2 Select the policy that you want to authorize.

3 Add **edpa.exe**, **wdp.exe**, **vfsmd.sys**, and **vrtam.sys** to the authorized files list. This procedure should be done for both **Suspicious Files** and **Suspicious Behavior** sections.

4 Click the **Checksum** tab and add the checksum file.

5 Click **OK**.

See "About Sophos Enterprise Console and Symantec DLP Agent" on page 63.

Configuring Sophos Application Control to work with Symantec DLP Agent (server-side)

You must configure Sophos Application Control to work with Symantec DLP Agent

To configure Sophos Application Control

1 On the console home page, click the **Application Control** option under the Policies section.

2 Select the policy that you want to authorize.

3 Add **edpa.exe**, **wdp.exe**, **vfsmd.sys**, and **vrtam.sys** to the authorized files list. This procedure should be done for both **Suspicious Files** and **Suspicious Behavior** sections.

4 Click **OK**.

See "About Sophos Enterprise Console and Symantec DLP Agent" on page 63.

Configuring Symantec Critical System Protection to work with Symantec DLP Agent (server-side)

The default Prevention Policy that is used in Symantec Critical System Protection prohibits the Symantec DLP Agent from operating. Follow these steps to create a custom policy that enables full access for the Symantec DLP Agent.

To create a custom policy that allows full access for edpa.exe

1. Access the server on which Symantec Critical System Protection is installed.
2. Select **Start > Programs > Symantec Critical System Protection > Management Console**.
3. Enter the administrator user name and password, and select **SCSPServer** from the **Server** menu. Click **Login** to proceed.
4. Select the **Prevention View** tab.
5. On the left-hand side, click the **Policies** icon.
6. Click the **+** icon on the right-hand side to start the **New Policy Wizard**.
7. Enter a name for the new policy in the **Name** field. For example: Vontu Agent Core.
8. Select **Windows** from the **Operating System** menu.
9. Select **All** from the **Policy Pack** menu.
10. Select **sym_win_protection_core_sbp** from the list of starting policies.
11. Click **Next** to load the starting policy values.
12. Click **Next** on each of the following New Policy Wizard screens to accept default values:
    - **Disable Prevention**
    - **Configure Inbound Network Access**
    - **Configure Outbound Network Access**
    - **Configure Outlook Attachments**
    - **Give Programs Extra Privileges**
    - **Give Users Extra Privileges**
    - **Give Groups Extra Privileges**
13. On the Allow users to override the policy screen, select **Allow ALL users to override the policy** and then click **Next**.
14. Click **Next** on each of the following New Policy Wizard screens to accept default values:

- **Allow users to run the agent configuration tools**
- **Allow users to run the Agent Event Viewer**

15 On the Set Policy Summary screen, click **Finish** to save the policy and complete the **New Policy Wizard**.

16 In the list of available policies, right-click the policy you created, and select **Edit Policy**.

17 Select **My Custom Programs** on the left-hand side of the policy screen.

18 Click **New** to add a new custom program.

19 Enter a name for the custom program in the **Display Name** field. For example: DLP.

20 Select **This Program is a service** from the **Category** menu.

21 In the **Identifier** field, type the text: edpa. Then click **Finish** to add the custom control.

22 On the left-hand side of the screen, select **My Custom Programs > *DLP* > Settings** where *DLP* is the name of the custom program you created.

23 On the right-hand side of the screen, select ***DLP*** **> Specify Services with Custom privileges > List of custom services**.

24 Click **Add** to add a custom service.

25 In the Program Path field, enter the full path to the `edpa.exe` service. The default path is `c:\Program Files\Manufacturer\Endpoint\edpa.exe`.

26 Click **OK** to add the program path.

27 Ensure that the following options are selected (checked):

- **Specify Services with Custom privileges**
- **Disable prevention -- Log but don't prevent policy violations**
- **Block modifications to executable files**
- **Block registration of COM and ActiveX controls**
- **Enable Buffer Overflow Detection**

28 Uncheck the following options:

- **Enable logging of trivial policy violations**
- **Enable Thread Injection Detection**

29 Click **Apply** and then click **OK** to save your changes to the policy.

30 To use the new policy, right-click its name in the policy list and select **Apply Policy**. Then select the computers on which to apply the policy.

See also your Symantec Critical System Protection documentation.

Symantec DLP Agent and client-side application configuration

The Symantec DLP Agent interoperates with a wide variety of other client-side applications such as antivirus, firewall, and other security applications. The following sections describe some commonly used applications to which you must make some minor adjustments to ensure that the Symantec DLP Agent works correctly. The third-party clients that are affected are:

- Symantec Endpoint Protection versions 11 and 12
  See "Configuring Symantec Endpoint Protection (SEP) to work with the Symantec DLP Agent (client-side)" on page 68.
- Symantec AntiVirus 9.0
  See "Configuring Symantec AntiVirus 9.0 to work with Symantec DLP Agent (client-side)" on page 67.
- Trend Micro PC-cillin 2007 v15.30
  See "Configuring Trend Micro PC-cillin 2007 v15.30 to work with Symantec DLP Agent (client-side)" on page 68.
- Sophos Anti-virus and Firewall V7.6.1 R2
  See "Configuring Sophos Anti-virus and Firewall to work with Symantec DLP Agent (client-side)" on page 69.
- McAfee Total Protection Service Firewall
  See "Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side)" on page 70.
- McAfee VirusScan
  See "Configuring McAfee VirusScan to work with Symantec DLP Agent (client-side)" on page 70.

Configuring Symantec AntiVirus 9.0 to work with Symantec DLP Agent (client-side)

Symantec AntiVirus 9.0 registers the Symantec DLP Agent as a medium-level threat. The software attempts to block the installation of the Symantec DLP Agent with a pop-up error message.

To configure Symantec AntiVirus 9.0

- From the installation error pop-up message during the Symantec DLP Agent installation, select **Permit Always**.

Configuring Symantec Endpoint Protection (SEP) to work with the Symantec DLP Agent (client-side)

The Symantec DLP Agent can appear to Symantec Endpoint Protection (SEP) software as if it were a virus. If your endpoint computers use Symantec Endpoint Protection version 11 or 12, you must exclude the `kvoop.exe` file from antivirus scans. This file is used by the Symantec DLP Agent. All other files that are used by the DLP Agent are digitally signed by Symantec and do not trigger virus-prevention actions in SEP. The file is in the following location:

<agent installation directory>`\Verity`

Where *<agent installation directory>* is the path to the agent installation directory. This path is configurable when you install the agent. The default path is: `C:\Program Files\Manufacturer\Endpoint Agent`.

For more information on excluding the file, see the following article on the Symantec Support Web site: "Excluding a file or folder from scans". (http://www.symantec.com/business/support/index?page=content&id=HOWTO55205#v39818564).

Configuring Trend Micro PC-cillin 2007 v15.30 to work with Symantec DLP Agent (client-side)

Trend Micro reports `edpa.exe` and `CUI.exe` as suspicious applications and blocks them. You must add `edpa.exe` and `CUI.exe` to the Trend Micro Exception List.

To configure Trend Micro PC-cillin 2007 v15.30

1. From the main console menu, open the **Prevent Unauthorized Changes** menu.
2. From the Virus & Spyware Controls option, click **Exception List**.
3. Click **Add Program**.
4. Add `edpa.exe` and `CUI.exe` to the list of acceptable programs.
5. Select **Trust** from the response drop-down menu.
6. Click **Save**.

Configuring Sophos Anti-virus and Firewall to work with Symantec DLP Agent (client-side)

Three configuration changes are required to ensure that the Symantec DLP Agent works correctly with Sophos Anti-virus and Firewall V7.6.1R.

First, Sophos Anti-virus reports `edpa.exe` and `wdp.exe` as suspicious programs at the time of agent installation. You must configure Sophos to ignore the Symantec DLP Agent.

Configuring Sophos to ignore the Symantec DLP Agent:

1. Open Sophos Anti-virus.
2. Open the **Configure Sophos Anti-Virus** menu option.
3. Select the **Authorization** menu option.
4. In the **Authorization Manager** window, select the **Buffer overflow** tab.
5. Find the `edpa.exe` and `wdp.exe` programs that have been blocked and move them to the **Authorized list**.
6. Click **OK**.

Second, Sophos Anti-virus reports drivers `vfsmfd.sys` and `vrtam.sys` as suspicious program. You must configure Sophos to accept these SYS files as valid files.

Configuring Sophos to accept Symantec DLP Agent drivers:

1. Open Sophos Anti-virus.
2. Open the Configure Sophos Anti-virus menu option.
3. Select the Authorization menu option.
4. In the **Authorization Manager** window, select the **Buffer overflow** tab.
5. Find the `vfsmfd.sys` and `vrtam.sys` files that have been blocked and move them to the **Authorized list**.
6. Click **OK**.

Third, Sophos firewall blocks access when the Symantec DLP Agent initiates communication with the Endpoint Server. You must allow the `edpa.exe` application access to the network.

Configuring the Sophos firewall to allow Symantec DLP Agent to access the network:

1. On the pop-up warning window, select the **Add the checksum to existing checksums for this application option.**
2. Click **OK.**

Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side)

By default, McAfee Total Protection Service blocks the Symantec DLP Agent (`edpa.exe`) from communicating with the Endpoint Server. If you already installed McAfee Total Protection Service on a client computer, configure the client firewall to allow full access for `edpa.exe`.

If you have not yet installed McAfee Total Protection Service, create a default server policy that gives full access to `edpa.exe` during installation.

See "To create a custom server policy for edpa.exe access" on page 62.

To configure the McAfee Total Protection Service client firewall

1. In the taskbar, right-click the icon for McAfee Total Protection Service and select **Firewall Settings**.
2. Select the **Internet Applications** tab.
3. Select the `edpa.exe` application in the **Internet Applications** list, then select the **Full Access** option in **Permissions**.
4. Click **OK**.
5. Restart all Windows services that are associated with McAfee Total Protection Service.

Configuring McAfee VirusScan to work with Symantec DLP Agent (client-side)

McAfee VirusScan in Maximum Protection Mode prevents installation of the Symantec DLP Agent. Follow these steps to add the necessary Symantec DLP Agent executables to the exclusion list in the McAfee VirusScan Console.

To configure McAfee VirusScan to work with Symantec DLP Agent

1. Open the McAfee VirusScan Console.
2. Open the **Access protection properties** panel.
3. Select **Common Maximum Protection** and click **edit**.
4. In the **Prevent program registering as service** folder, add the following executables to the exclusion list: `edpa.exe`, `wdp.exe`, and `services.exe`.
5. In the **Prevent creation of new executable files in Windows** folder, add the following executables to the exclusion list: `AgentInstall.msi`, `edpa.exe`, and `wdp.exe`.

6 In the **Prevent creation of new executable files in Program files** folder, add the following executables to the exclusion list: `AgentInstall.msi`, `edpa.exe`, and `wdp.exe`.

7 Click **Apply** to apply your changes.

Configuring Symantec NetBackup 6.5 to work with Windows Vista

Symantec NetBackup fails to back up and restore after Symantec DLP Agent is installed on Windows Vista. The master server returns "Error code 23: A read operation from a socket failed, to NetBackup client." The server's administrative console displays "Error code 25," which is related to time-out settings under the respective Windows Vista client section.

To configure Symantec NetBackup 6.5

- Make sure that you have installed Microsoft Windows Vista Service Pack 1.

  To download Service Pack 1, go to: `http://support.microsoft.com/` and search for Windows Vista SP1.

The Symantec DLP Agent requires Service Pack 1 on Microsoft Windows Vista computers. If you do not install Service Pack 1, you must manually restart NetBackup 6.5 after the Symantec DLP Agent starts on each endpoint computer.

Chapter 4

Symantec Data Loss Prevention Mobile Prevent Compatibility and Information

This chapter includes the following topics:

Symantec Data Loss Prevention for Mobile compatibility

The following table lists the iOS applications and response rules that are supported by Mobile Prevent. See the *Symantec Data Loss Prevention Administration Guide* for more information on creating policies and response rules.

Note: Applications for iOS are frequently updated. The following table lists the application versions that have been verified for functionality with Mobile Prevent.

Table 4-1 Applications, iOS devices, and response rules supported by Mobile Prevent

Application	Device	Block response rule	Content Removal response rule
Dropbox version 1.4.7	iPad iPhone	Yes	Yes
Facebook with chat version 4.0.3 **Note:** Chat feature is not supported.	iPhone iPad	Yes	Yes
Gmail version 1.1 **Note:** Note: Supported only for monitoring.	iPad iPhone	No	No
Goodreader version 3.12.0 **Note:** FTP support only.	iPad	Yes	Yes
ActiveSync (iOS native email) **Note:** Microsoft Exchange 2003 and 2007 Support	iPad	Yes	Yes
ActiveSync (iOS native email) **Note:** Microsoft Exchange 2003 and 2007 Support	iPhone	Yes	No

Mobile Prevent supports the following Web applications through the Safari Web browser for iPads and iPhones (for iOS versions 4.3.4, 5.0, 5.0.1, 5.1, and 5.1.1). This table also lists the supported type of response rules available for each Web application. See the *Symantec Data Loss Prevention Administration Guide* for more information on creating policies and response rules.

Table 4-2 Web applications and response rules supported by Mobile Prevent

Application	Block response rule	Content Removal response rule
AOL	Yes	Yes

Table 4-2 Web applications and response rules supported by Mobile Prevent *(continued)*

Application	Block response rule	Content Removal response rule
Facebook	Yes	Yes
Gmail	No	No
Windows Live Mail	Yes	Yes
Yahoo! Mail	Yes	Yes
Twitter	Yes	No

The following iOS components and applications are not supported in this release of Symantec Data Loss Prevention Mobile Prevent:

- SMTP and IMAP messaging
- iCloud functionality
- iTunes wireless synchronization

  Note: iTunes synchronization is supported using a USB cable. See the documentation that comes with your mobile device for more information.

- Netflix for iPad application

About using Symantec Data Loss Prevention for Mobile with iPad and iPhone applications

In some cases you might need to configure the application or the network environment to enable an application to function properly. The most common adjustments fall into two these categories:

- Server-side
  See "Symantec Data Loss Prevention Mobile Prevent and server-side application configuration" on page 76.
- Client-side
  See "Symantec Data Loss Prevention Mobile Prevent and client-side application configuration" on page 79.

The following sections provide instructions to enable third-party applications to work with Symantec Data Loss Prevention for Mobile. Other applications that are not listed in these sections may also require changes to permit the application to function. In these cases, refer to your third-party application documentation.

Symantec Data Loss Prevention Mobile Prevent and server-side application configuration

You must make a few configuration changes to a number of server products. If you do not make these changes, the mobile devices that are connected to the corporate network might not function properly. The server products that are affected are:

- Streaming applications
  See "Configuring streaming applications to work with Symantec Data Loss Prevention for Mobile" on page 76.
- Netflix
  See "Netflix streaming with Symantec Data Loss Prevention Mobile Prevent" on page 77.
- Gmail
  See "Configuring Gmail on iPads or iPhones with Symantec Data Loss Prevention Mobile Prevent" on page 78.

Configuring streaming applications to work with Symantec Data Loss Prevention for Mobile

To enable some streaming applications, such as Pandora, a proxy server must be configured to redirect network traffic. The proxy server can be configured to allow communication between the mobile device and the streaming server. This configuration prevents Symantec Data Loss Prevention for Mobile from scanning the streaming data.

Configuring the proxy server to redirect network traffic

1. Log in to the proxy server.
2. Create a forwarding rule that includes the URL or IP addresses of the streaming Web sites that you want users to access.
3. Disable SSL interception in the rule.
4. Save the rule.

For more information on configuring the proxy server, see the documentation that comes with the proxy server.

Netflix streaming with Symantec Data Loss Prevention Mobile Prevent

Netflix is not supported on a mobile device in a Symantec Data Loss Prevention Mobile Prevent environment. Configuring the proxy server to redirect communication to the Netflix servers allows Netflix to stream movies to the mobile device. The streaming data is not scanned by Mobile Prevent.

Configuring the proxy server to redirect network traffic

1. Log in to the proxy server.
2. If the proxy server is configured for explicit mode, create a forwarding rule for the destination host `netflix`.
3. If the proxy server is configured for transparent mode, create a forwarding rule for the destination host `amazonaws.com`.
4. Disable SSL interception in the rule.
5. Save the rule.

If users are restricted from using Netflix to stream videos, the proxy server can be configured to block communication between the proxy server and Netflix. This configuration can be used to increase performance in the corporate network. For more information on configuring the proxy server, see the documentation that comes with the proxy server.

YouTube streaming with Symantec Data Loss Prevention Mobile Prevent

If the proxy server is configured for transparent mode, YouTube videos may not play. To enable YouTube videos on mobile devices connected through a VPN, create a new policy on the proxy server for the YouTube host.

Note: The following procedure is an example of installing a new policy on a Blue Coat proxy server. See the documentation for your proxy server for more information on how to create a policy.

Configuring the proxy server for YouTube

1. Log in to the proxy server as an administrator.
2. Click **Configuration > Policy > Policy Files**.
3. From the **Install Local Policy from list** menu, click **Text Editor**.

4 In the field provided, enter the following:

```
define condition YouTubeRangeRequests
    url.domain="YouTube.com"
end condition YouTubeRangeRequests
<Proxy>
    request.header.Range="bytes" condition=YouTubeRangeRequests
bypass_cache(yes)
```

5 Click **Apply** to save the policy.

Configuring Gmail on iPads or iPhones with Symantec Data Loss Prevention Mobile Prevent

Symantec Data Loss Prevention for Mobile can use notification and block response rules when an email is sent that violates a policy. To use the block response rule, an iOS device is configured to use Gmail-based email through the Google Sync server. The user must use the native iOS Mail application to send their emails instead of using the Gmail mail application. If a user sends emails with the Gmail application, only the notification response rule can be used when an email violates a policy.

Note: Symantec Data Loss Prevention for Mobile does not support block response rules for any emails that are sent using the Gmail application on iOS mobile devices. The Gmail application might become unusable if the application is used to send an email that gets blocked by the Mobile Prevent Server. To correct this problem, remove the response rule to block the emails and then reinstall the Gmail application on the mobile device.

To configure Gmail with the native iOS Mail application, complete the following steps.

1 From the Home screen, tap **Settings**.

2 Tap **Mail, Contacts, Calendars** > **Add Account** > **Microsoft Exchange**.

Note: Do not use the Gmail account that is displayed in the list of account types.

---

3 Enter the following information into the fields provided.

Email	*username@gmail.com*
Server	**m.google.com**
Domain	*gmail.com* (Optional)
Username	*user name*
Password	*password*

4 Tap **Next** > **Save** to save the account.

The user can now use the native iOS Mail application on their mobile device to send and receive emails from their Gmail account. The Mobile Prevent Server can monitor and generate notification or block response rules when an email containing sensitive data is detected.

Symantec Data Loss Prevention Mobile Prevent and client-side application configuration

Some applications might require changes to their settings to allow them to function properly in the Symantec Data Loss Prevention for Mobile environment. If you do not make these changes the applications may not function properly. The known applications that are affected are:

- iOS updates
  See "Configuring iOS updates to work with Symantec Data Loss Prevention Mobile Prevent" on page 79.
- Twitter
  See "Using Twitter with Symantec Data Loss Prevention Mobile Prevent" on page 80.
- Facebook Chat

Configuring iOS updates to work with Symantec Data Loss Prevention Mobile Prevent

An iOS-based mobile device that is configured for VPN connectivity must perform any iOS updates while connected to the corporate network. Disabling the VPN connection and updating the iOS operating system might cause the update to fail.

Using Twitter with Symantec Data Loss Prevention Mobile Prevent

Users who send messages with Twitter might receive an authorization error after a message is sent. When the error occurs, the message is not sent or has had content removed due to content that violates a policy. The message creates an incident on the Symantec Data Loss Prevention Enforce Server. The user can continue to use Twitter to send messages.

Index

L

M

N

O

P

R

S

T

V

W

Y