Symantec™ Data Loss Prevention System Requirements and Compatibility Guide

Version 10.5

symantec™

1-1000-1050-2010-04-05

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.

Documentation version: 10.5

Legal Notice

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:

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 10.
- The system requirements for your Symantec Data Loss Prevention installation

See "The effect of scale on system requirements" on page 11.

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 database administration team.

If you choose this installation, the administrator needs to be able to perform database maintenance tasks, such as database backups.

See "System requirements for Symantec Data Loss Prevention servers" on page 12.

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 "System requirements for Symantec Data Loss Prevention servers" on page 12.

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 1-1 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 hardware requirements" on page 12.	See "Large/very large enterprise hardware requirements" on page 13.

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

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 hardware requirements" on page 12.
- See "Large/very large enterprise hardware requirements" on page 13.
- See "Operating system requirements for servers" on page 15.

Symantec Data Loss Prevention requires the Oracle 10g database. 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 21.

All installations that include the Endpoint Discover or Endpoint Prevent products require a separate Symantec Management Console installation, which has its own set of system requirements.

See "About Symantec Management Platform server requirements" on page 19.

Small/medium enterprise hardware requirements

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

Table 1-2 Small/medium enterprise system requirements

Required for	Enforce	Network Monitor	Discover/Prevent/Endpoint
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 10g.	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 0+1 configuration is recommended with four main drives, 1 redundant	140 GB Ultra SCSI	140 GB Ultra SCSI

Table 1-2 Small/medium enterprise system requirements *(continued)*

Required for	Enforce	Network Monitor	Discover/Prevent/Endpoint
NICs	To communicate with detection servers: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC	To communicate with Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC For network traffic monitoring (pick one): 1 copper or fiber 1 Gb/100 Mb Ethernet NIC. or Endace network measurement card to monitor network traffic. This card is optional, but improves detection performance in high-traffic environments. Supported cards: EDM01-01v7_DAG_3.7 EDM01-01v7_DAG_4.3GE DAG_4.5 G2/G4 (PCI-X) DAG_7.5 G2/G4 (PCI-E) See See Table 1-10 on page 27.	To communicate with Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC

See “The effect of scale on system requirements” on page 11.

Large/very large enterprise hardware requirements

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

Table 1-3 Large/Very Large enterprise system requirements

Required For	Enforce	Network Monitor	Discover/Prevent/Endpoint
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

Table 1-3 Large/Very Large enterprise system requirements *(continued)*

Required For	Enforce	Network Monitor	Discover/Prevent/Endpoint
Memory	8–16 GB RAM (EDM/IDM size can increase memory requirements) Two-tier deployments require additional memory for running Oracle 10g.	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 0+1 configuration is recommended with four main drives, 1 redundant	140 GB Ultra SCSI	140 GB Ultra SCSI
NICs	To communicate with detection servers: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC	To communicate with Enforce: 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. or Endace network measurement card to monitor network traffic. This card is optional, but improves detection performance in high-traffic environments. Supported cards: EDM01-01v7_DAG_3.7 EDM01-01v7_DAG_4.3GE DAG_4.5 G2/G4 (PCI-X) DAG_7.5 G2/G4 (PCI-E) See See Table 1-10 on page 27.	To communicate with Enforce: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC

See “The effect of scale on system requirements” on page 11.

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.

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

- Microsoft Windows Server 2003, Enterprise Edition (32-bit) with Service Pack 2 or higher
- Red Hat Enterprise Linux 5 (32-bit) Update 2 or higher

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. Note that localized Linux platforms are not currently supported.

See “Supported languages for detection” on page 17.

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

See “System requirements for Symantec Data Loss Prevention servers” on page 12.

Linux partition size guidelines

Minimum size 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.

Table 1-4 Linux partition minimum size guidelines—Enforce Server with Oracle database

Partition	Minimum size guidelines	Description and Comments
/	30 GB minimum 40 GB recommended to accomodate future expansions and upgrades	The Oracle installer requires significant space in this directory.
/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.

Table 1-4 Linux partition minimum size guidelines—Enforce Server with Oracle database *(continued)*

Partition	Minimum size guidelines	Description and Comments
`/var`	15 GB for Small/Medium installations 45 GB for Large/Very Large installations	
`/boot`	100 MB	This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported).
swap	8 GB if RAM equal 8 GB or less Equal to RAM if RAM is between 8 and 16 GB 16 GB if RAM is equal or greater than 16 GB	If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts.

Table 1-5 Linux partition minimum size guidelines—Enforce Server without an Oracle database

Partition	Minimum size guidelines	Description and Comments
`/`	30 GB minimum 40 GB recommended to accomodate future expansions and upgrades	
`/opt`	10 GB	Contains installed programs such as Symantec Data Loss Prevention and the Oracle client.
`/var`	15 GB for Small/Medium installations 45 GB for Large/Very Large installations	Contains logs and any EDM/IDM indexes.
`/boot`	100 MB	This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported).
swap	8 GB if RAM is 8 GB or less Equal to RAM if RAM is between 8 and 16 GB 16 GB if RAM is equal or greater than 16 GB	If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts.

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

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
- Microsoft Windows Vista Enterprise or Business with Service Pack 1
- Microsoft Windows 7 (32-bit or 64-bit), Enterprise, Professional, or Ultimate

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

See "Supported languages for detection" on page 17.

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 38.

See "About Symantec Management Platform server requirements" on page 19.

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 1-6 Languages supported by Symantec Data Loss Prevention

Language	Version 9.x	Version 10.0	Version 10.5
Arabic	Yes	Yes	Yes
Brazilian Portuguese		Yes	Yes
Chinese (traditional)	Yes	Yes	Yes
Chinese (simplified)	Yes	Yes	Yes
Czech		Yes	Yes
Danish	Yes	Yes	Yes
Dutch	Yes	Yes	Yes
English	Yes	Yes	Yes

Table 1-6 Languages supported by Symantec Data Loss Prevention *(continued)*

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

* Content written in Turkish can be inspected for policy violations. Symantec Data Loss Prevention cannot be installed on a Windows operating system that is localized for the Turkish language. Turkish cannot be chosen 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 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 UI.
- 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.

About Symantec Management Platform server requirements

All installations that include the Endpoint Discover or Endpoint Prevent products require a separate Symantec Management Platform 7.0 (SP2 or later) installation. Symantec Management Platform 7.0 SP3 is required to support Windows 7 endpoint computers.

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

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

System requirements for Symantec Management Platform

Use Symantec Installation Manager to install the Symantec Management Platform products. During the installation process, Symantec Installation Manager displays an **Install Readiness Check** page. On this page, Symantec Installation Manager verifies many of the following system requirements.

For more information, see Symantec Management Platform Capacity Planning and Altiris 7 Planning and Implementation Guide at the following URLs:

https://kb.altiris.com/article.asp?article=45597&p=1

https://kb.altiris.com/article.asp?article=45803&p=1

Table 1-7 Hardware requirements and recommendations

Hardware	Minimum requirements for evaluation	Recommended for small business	Recommended for large enterprise
CPU	Pentium 4	Dual processor dual core	Dual processor quad core
CPU Speed	1.8 GHz	2.53 GHz	2.53 GHz
RAM	1 GB	4 GB, DDR2	8 GB, DDR2
Cache	not checked	3 MB L2	6 MB L2
Network	not checked	Gigabit	Gigabit
Hard disk	5 GB of free disk space	10,000 RPM SCSI or better. 10 GB of free disk space.	10,000 RPM SCSI for RAID 1, 4, or 10. Additional space dependent on implementation of site services, Software Library, and other considerations.

Table 1-8 Software requirements and recommendations

Software	Minimum requirements for evaluation	Recommended for small business	Recommended for large enterprise
Microsoft.NET	Microsoft.NET 3.5	Microsoft.NET 3.5	Microsoft.NET 3.5
Microsoft Operating system	Microsoft Windows Server 2003 (Windows Server 2008 is not supported.)	Microsoft Windows Server 2003 (Windows Server 2008 is not supported.)	Microsoft Windows Server 2003. (Windows Server 2008 is not supported.)

Table 1-8 Software requirements and recommendations *(continued)*

Software	Minimum requirements for evaluation	Recommended for small business	Recommended for large enterprise
Web browser	Microsoft IE 7 or IE 8	Microsoft IE 7 or IE 8	Microsoft IE 7 or IE 8
Microsoft IIS	IIS 6	IIS 6	IIS 6
AJAX	AJAX 1.0	AJAX 1.0	AJAX 1.0
Microsoft SQL Server	Microsoft SQL Server 2005 Express	Microsoft SQL Server 2005 Express for 500 or less managed computers. Microsoft SQL Server 2005 Standard or Enterprise for more than 500 managed computers.	Microsoft SQL Server 2005 Enterprise. Use the following configuration guidelines: ■ Virtual disk 1: Operating system and SQL Server (RAID 1, 5, or 10) ■ Virtual disk 2: Data (36 GB minimum disk size) ■ Virtual disk 3: Logs (36 GB minimum disk size) ■ Virtual disk 4: Temp db (36 GB minimum disk size) The SQL Server database for large environments with managed computers, software, and multiple solutions can grow to 15 GB. See Microsoft SQL Server best practices for disk, file growth, and maintenance strategies.

Oracle database requirements

Symantec Data Loss Prevention requires the Oracle 10g database version 10.2.0.4 with the most recent Critical Patch Update. Symantec Data Loss Prevention includes both Oracle 10g and the necessary patches. Oracle can be run on Windows Server 2003 (any 32-bit version) and Red Hat Enterprise Linux (any 32-bit version) operating systems. Note that Symantec Data Loss Prevention supports only the Data Loss Prevention schema that is included with the software distribution.

See the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide* for information about installing or upgrading Oracle software.

You can install Oracle 10g 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 10g Client on the Enforce Server computer to communicate with the remote Oracle 10g 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 hardware requirements" on page 12.
  See "Large/very large enterprise hardware requirements" on page 13.

If you install Oracle 10g on a dedicated server, that computer must meet the following minimum system requirements:

- Microsoft Windows Server 2003 or Red Hat Enterprise Linux version 5 Update 2, or later version of 5.x (32-bit)
- 6 GB of RAM
- 6 GB of swap space
- 300–500 GB of disk space for the Enforce database

On a Linux system, if the Oracle database is on the same computer as the Enforce Server, then the `/opt` file system should have at least 500 GB of free space. If Oracle is installed on a different computer from the Enforce Server, then the `/opt` file system should have at least 300 GB of free space. The `/boot` file system should have at least 20 GB of free space.

The minimum disk space requirement applies only to the Enforce database. Additional disk space (approximately 300 GB) is required for the Oracle 10g software and for general management tasks such as backups and log files. See the Oracle 10g documentation for more information.

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 2.x or 3.x.

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

- Microsoft Internet Explorer 6.x, 7.x, or 8.x
- Mozilla Firefox 2.x or 3.x

Note: You must install a Microsoft Language Pack on a Windows client system to support certain languages.

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

Virtual server and virtual workstation support

Symantec supports running the following server components on VMware ESX version 3.5 virtual machines instead of dedicated server hardware:

- Enforce Server
- Network Discover
- Network Protect
- Network Prevent Server (Email)
- Network Prevent Server (Web)

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 Endpoint Prevent detection server on virtual hardware.

See "System requirements for Symantec Data Loss Prevention servers" on page 12.

Symantec supports running the Symantec DLP Agent software on virtual workstations using VMware Workstation 6.5.x.

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.

Individual Citrix clients do not require a Symantec DLP Agent installation to support this functionality. However, because a single Symantec DLP Agent installation monitors multiple Citrix clients, you must purchase an Endpoint Prevent license that covers all of your Citrix clients. See your Symantec sales representative for more information.

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 1-9 Citrix virtualization support and limitations

Supported Citrix product	Endpoint Prevent use case	Limitations
Citrix XenApp 4.5 on Windows Server 2003 (32-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 26. ■ 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 1-9 Citrix virtualization support and limitations *(continued)*

Supported Citrix product	Endpoint Prevent use case	Limitations
Citrix XenDesktop 3.0 with Windows XP, Windows Vista (32-bit), or Windows 7 (32-bit or 64-bit) guest operating systems.	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 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 1-10 for required software
- Table 1-11 for required Linux RPMs
- Table 1-12 for recommended software

Table 1-10 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 5.5.27	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_14	All servers	The Symantec DLP Installation Wizard automatically installs the correct JRE version.
WinPcap 4.0.2	Required for Windows-based Network Monitor Server. Recommended for all Windows-based detection servers.	Windows packet capture library. Download from winpcap.org.
Endace card driver 3.3.1	Detection servers equipped with an Endace network measurement card.	Download from Endace. See "Small/medium enterprise hardware requirements" on page 12.

Table 1-10 Required third-party software *(continued)*

Software	Required for	Description
VMware ESX version 3.5	Required to run supported components in a virtualized environment. See "Virtual server and virtual workstation support" on page 23.	Virtualization software. Download from vmware.
Windows Services for UNIX Version 3.5 (SFU35SEL_EN.exe)	Required for any Network Discover Server that runs scans on a UNIX or Linux computer.	Download from the Microsoft Download Center - SFU.

In addition to the Linux Minimal Installation, Linux-based Symantec Data Loss Prevention servers require the Red Hat Package Managers (RPM) listed in Table 1-11

Table 1-11 Required Linux RPMs

Linux-based servers	Required RPMs

Enforce Server
Oracle server
	`gcc`
	`cpp`
	`compat-libstdc++-296`
	`compat-libstdc++-33`
	`glibc-devel`
	`glibc-kernheaders`
	`binutils`
	`Xorg-x11*`
	`vim`
	`emacs`

Network Monitor Server	`compat-libstdc++-296`
	`compat-libstdc++-33`
	`vim`
	`libX11`
	`Xorg-X11-Auth`

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

Table 1-12 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.

Product compatibility

This chapter includes the following topics:

Environment compatibility and requirements for Network Prevent (Email)

The Network Prevent Server (Email) 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 Server (Email) 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 Server (Email) in reflecting mode, the upstream MTA must be able to route messages to the Network Prevent Server (Email) 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 Server (Email). For reflecting mode compatibility, the MTA must also be able to route messages that are returned from the Network Prevent Server (Email) out to their intended recipients.

Network Prevent Server (Email) 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 Network Prevent Server (Email). Successful authentication requires that the appropriate keys and X509 certificates are available for each mail server in the proxied message chain.

Proxy server compatibility with Network Prevent (Web)

Network Prevent Servers (Web) can operate with the following HTTP proxies:

Table 2-1 Network Prevent Server (Web) Supported proxy servers

Proxy	Supported Protocols	Configuration Information
Blue Coat ProxySG	HTTP, HTTPS, FTP over HTTP, or FTP proxy	Blue Coat product documentation
Blue Coat NetCache proxy	HTTP, FTP over HTTP	
Cisco IronPort S-Series	HTTP, HTTPS, FTP over HTTP	Cisco IronPort product documentation
Microsoft ISA	HTTP, limited FTP over HTTP	See the *Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server*
Secure Computing Secure Web (Webwasher)	HTTP, HTTPS, FTP over HTTP or FTP proxy	Secure Web documentation (particularly the chapter that describes setting up Secure Web with a DLP Solution)
Squid Web Proxy	HTTP	See the *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy*

Network interfaces to third-party software and servers

Symantec Data Loss Prevention uses the following network protocols and interfaces to connect with third-party servers and network equipment:

Table 2-2 Network interfaces and configurations

Interface	Specific Version/Configuration	Version 9.x	Version 10.x
802.x	Top Layer switch with Endace	Yes	Yes
SMTP	Any MTA in compliance with ESMTP as defined in RFC 2821; MTA must be able to route messages to the Network Prevent (Email) server once and only once for each message.	Yes	Yes
SQL	Oracle	Yes	Yes
ICAP	Blue Coat (Web Proxy)	Yes	Yes
ICAP	Webwasher (Web Proxy)	Yes	Yes
ICAP	Squid (Web Proxy)		Yes
ICAP	Ironport S-Series Web Security Appliance (Web Proxy)		Yes
ICAP	MS ISA 2004, 2006 Standard and Enterprise Edition can be integrated using the ICAP interface provided by the Symantec Data Loss Prevention ISA Web filter. See the *Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server*.		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 share targets" on page 34.

See "Supported Lotus Notes targets" on page 35.

See "Supported SQL database targets" on page 35.

See "Supported Exchange (scanner) targets" on page 36.

See "Supported file system (scanner) targets" on page 35.

See "Supported Exchange (scanner) targets" on page 36.

See "Supported SharePoint targets" on page 37.

See "Supported Documentum (scanner) targets" on page 38.

See "Supported Livelink (scanner) targets" on page 38.

See "Supported Web server (scanner) targets" on page 38.

Supported file share targets

The File Systems (Server) target supports scanning of the following network file shares:

- CIFS on Windows
- NFS on Linux
- DFS on Windows 2003
  Preserving the last-accessed date on DFS shares requires additional setup.

In addition, the File Systems (Server) target supports scanning of the following file types:

- Microsoft Outlook Personal Folders (`.pst` files) created with Outlook 1997-2002, 2003, and 2007.
  The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2003 SP3 or later must be installed there.
- File systems on UNIX systems can also be scanned, even if they are not exposed as CIFS or NFS shares.
  Use the SFTP protocol to provide a method similar to the scans of file shares. Contact Symantec Professional Services for details.

You can also scan the local file system on a Linux Network Discover Server by listing the path name in the content root. For example, you can enter `/home/myfiles`.

Supported Lotus Notes targets

The Lotus Notes target supports scanning of the following versions:

- Lotus Notes 6.5
- Lotus Notes 7
- Lotus Notes 8

Both DIIOP and native configuration options are supported. Native mode is recommended, and a Lotus Notes client must be installed on the Network Discover Server.

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 6.5 has a manifest version in the JAR file of 1.3.1
- 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 file system (scanner) targets

The following remote Windows systems can be scanned:

- Windows 2000
- Windows 2003
- Windows XP, 32-bit

The following Linux file systems can be scanned:

- x86 32-bit, Red Hat Enterprise Linux AS 4

The following AIX file systems can be scanned:

- AIX 5.3

AIX requires the following C run time libraries, as well as Java 1.5:

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

The following Solaris file systems can be scanned:

- Solaris SPARC 8
- Solaris SPARC 9
- Solaris SPARC 10

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 machine 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 email message text and email 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, such as the following data objects:

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

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.

Supported SharePoint 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_10.5.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, 64-bit, or Windows 2008 R1

  Separate scanner installation is available for SharePoint 2007 64-bit servers. Use the following SharePoint scanner installation file for SharePoint 2007 64-bit servers.

  `SharePoint2007Scanner_windows_x64_10.5.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 38.

See “Endpoint Prevent supported applications” on page 39.

Endpoint Data Loss Prevention supported operating systems

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

Table 2-3 Endpoint Data Loss Prevention supported operating systems

Operating system	Version	Symantec Data Loss Prevention		
		Version 9.x	Version 10.0	Version 10.5
Windows XP Professional	SP2	Yes	Yes	Yes
	SP3	Yes	Yes	Yes
Windows 2003 (32-bit)	SP1	Yes	Yes	No

Table 2-3 Endpoint Data Loss Prevention supported operating systems *(continued)*

Operating system	Version	Symantec Data Loss Prevention		
		Version 9.x	Version 10.0	Version 10.5
	SP2	Yes	Yes	Yes
	R2	Yes	Yes	Yes
Windows Vista Enterprise (32-bit)	unpatched	Yes	Yes	No
	SP1	Yes	Yes	Yes
Windows 7 (32-bit)		No	Yes	Yes
Windows 7 (64-bit)		No	No	Yes

Endpoint Prevent supported applications

The following applications are supported by Endpoint Prevent:

Table 2-4 Applications supported by Endpoint Prevent

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

Table 2-4 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention		
			Version 9.x	Version 10.0	Version 10.5
		8.1	Yes	Yes	Yes
		9.0	No	Yes	Yes
	MSN Messenger	8.1	Yes	Yes	Yes
		9.0 (14)	No	Yes	Yes
	AIM	5.9	Yes	Yes	Yes
		6.0	Yes	Yes	Yes
		6.1	Yes	Yes	Yes
		6.5	No	Yes	Yes
		6.8	No	Yes	Yes
		6.9	No	Yes	Yes
	AIM Pro	1.4	*Yes	Yes	Yes
		1.5	*Yes	Yes	Yes
Email	Outlook	2002	Yes	Yes	Yes
		2003	Yes	Yes	Yes
		2007	Yes	Yes	Yes
	Eudora		No	No	No
	Thunderbird		No	No	No
	Lotus Notes	6.5	No	No	Yes
		7.0	Yes	Yes	Yes
		7.0.2 Multiuser	No	No	Yes
		8.0	Yes	Yes	Yes
		8.5	No	Yes	Yes
FTP			Yes	Yes	Yes
CD/DVD	BsClip		Yes	Yes	Yes

Table 2-4 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention		
			Version 9.x	Version 10.0	Version 10.5
	Bs Recorder Gold		Yes	Yes	Yes
	BurnAware		Yes	Yes	Yes
	Cheetah Burner		Yes	Yes	Yes
	Command Burner		Yes	Yes	Yes
	CopyToDVD		Yes	Yes	Yes
	Creator10		Yes	Yes	Yes
	Deep Burner		Yes	Yes	Yes
	GEAR for Windows		Yes	Yes	Yes
	mkisofs		Yes	Yes	Yes
	Nero		Yes	Yes	Yes
	NeroStartSmart		Yes	Yes	Yes
	Roxio		Yes	Yes	Yes
	Roxio RecordNow		Yes	Yes	Yes
	Roxio5		Yes	Yes	Yes
	Roxio Mediahub		Yes	Yes	Yes
	Silent Night Micro Burner		Yes	Yes	Yes
	Star Burn		Yes	Yes	Yes

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

Symantec DLP Agent Compatibility With Other Applications

This chapter includes the following topics:

- About using Symantec DLP Agent with other applications
- Symantec DLP Agent and server-side application configuration
- Symantec DLP Agent and client-side application configuration
- Configuring Symantec NetBackup 6.5 to work with Windows Vista

About using Symantec DLP Agent with other applications

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

See "Operating system requirements for endpoint systems" on page 17.

While the agent generally works seamlessly with other applications, in some cases you need to configure an application to enable the agent to function properly. The most common adjustments and configurations fall into two categories:

- Server-side
  See "Symantec DLP Agent and server-side application configuration" on page 44.
- Client-side

See “Symantec DLP Agent and client-side application configuration” on page 51.

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 44.
- McAfee ePolicy Orchestrator 4.0
  See “Configuring McAfee ePolicy Orchestrator to work with Symantec DLP Agent (server-side)” on page 45.
- McAfee Total Protection Service
  See “Configuring McAfee Total Protection Service to work with Symantec DLP Agent (server-side)” on page 46.
- Sophos Enterprise Console
  See “About Sophos Enterprise Console and Symantec DLP Agent” on page 47.
- Symantec Critical System Protection
  See “Configuring Symantec Critical System Protection to work with Symantec DLP Agent (server-side)” on page 48.

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 53.

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 47.
- Sophos Firewall systems
  See "Configuring Sophos Firewall to work with Symantec DLP Agent (server-side)" on page 48.
- Sophos Application Control
  See "Configuring Sophos Application Control to work with Symantec DLP Agent (server-side)" on page 48.

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 47.

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 47.

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 AntiVirus 9.0
  See "Configuring Symantec AntiVirus 9.0 to work with Symantec DLP Agent (client-side)" on page 51.
- 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 51.
- 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 52.
- McAfee Total Protection Service Firewall
  See "Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side)" on page 53.

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 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 46.

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 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.

Index