Symantec™ Data Loss Prevention Standard System Requirements and Compatibility Guide

Version 11.6

Last updated: 13 September, 2012

Symantec

Symantec Data Loss Prevention Standard System Requirements and Compatibility Guide

Document version: 11.6d

Legal Notice

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

Technical Support 4

Chapter 1 System Requirements and Recommendations 9

About updates to Symantec Data Loss Prevention system requirements 10
About accessing the Symantec Data Loss Prevention Knowledgebase 10
Deployment planning considerations 11
About installation tiers 11
The effect of scale on system requirements 12
Single-tier server minimum requirements for Symantec Data Loss Prevention Standard 12
Minimum system requirements for two-tier and three-tier deployments 14
Two-tier and three-tier minimum server requirements for a small/medium enterprise 14
Two-tier and three-tier server minimum requirements for a large/very large enterprise 15
Operating system requirements for servers 16
Endpoint computer requirements for the Symantec DLP Agent 18
Operating system requirements for endpoint systems 18
Memory and disk space requirements for the Symantec DLP Agent 19
Symantec DLP Agent connectivity requirements 19
Supported languages for detection 20
Available language packs 22
Oracle database requirements 23
Browser requirements for accessing the Enforce Server administration console 25
Requirements for using certificate authentication for single sign-on 25
Virtual server and virtual workstation support 26
Virtual desktop and virtual application support with Endpoint Prevent 27
Detection server restriction for Symantec DLP Agents on Citrix XenApp 30

Third-party software requirements and recommendations 31

Chapter 2 Product compatibility 33

Symantec Veritas Cluster Server compatibility 33
About Endpoint Data Loss Prevention compatibility 33
Endpoint Data Loss Prevention supported operating systems 34
Endpoint Prevent supported applications 35

Chapter 3 Symantec DLP Agent Compatibility With Other Applications 39

About using Symantec DLP Agent with other applications 39
Symantec DLP Agent and server-side application configuration 40
Configuring Cisco CSA Management Center to work with Symantec DLP Agent (server-side) 40
Configuring McAfee ePolicy Orchestrator to work with Symantec DLP Agent (server-side) 41
Configuring McAfee Total Protection Service to work with Symantec DLP Agent (server-side) 42
About Sophos Enterprise Console and Symantec DLP Agent 43
Configuring Symantec Critical System Protection to work with Symantec DLP Agent (server-side) 45
Symantec DLP Agent and client-side application configuration 47
Configuring Symantec AntiVirus 9.0 to work with Symantec DLP Agent (client-side) 47
Configuring Symantec Endpoint Protection (SEP) to work with the Symantec DLP Agent (client-side) 48
Configuring Trend Micro PC-cillin 2007 v15.30 to work with Symantec DLP Agent (client-side) 48
Configuring Sophos Anti-virus and Firewall to work with Symantec DLP Agent (client-side) 49
Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side) 50
Configuring McAfee VirusScan to work with Symantec DLP Agent (client-side) 50
Configuring Symantec NetBackup 6.5 to work with Windows Vista 51

Index 53

Chapter 1

System Requirements and Recommendations

This chapter includes the following topics:

- About updates to Symantec Data Loss Prevention system requirements
- About accessing the Symantec Data Loss Prevention Knowledgebase
- Deployment planning considerations
- Single-tier server minimum requirements for Symantec Data Loss Prevention Standard
- Minimum system requirements for two-tier and three-tier deployments
- Endpoint computer requirements for the Symantec DLP Agent
- Symantec DLP Agent connectivity requirements
- Supported languages for detection
- Available language packs
- Oracle database requirements
- Browser requirements for accessing the Enforce Server administration console
- Requirements for using certificate authentication for single sign-on
- Virtual server and virtual workstation support
- Virtual desktop and virtual application support with Endpoint Prevent
- Third-party software requirements and recommendations

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 Standard System Requirements and Compatibility Guide* at the following link to the Symantec Data Loss Prevention Standard knowledgebase. You must be a licensed Symantec Data Loss Prevention Standard customer and have a login for the knowledgebase to access this article.

https://kb-vontu.altiris.com/article.asp?article=55644

Table 1-1 Change log

Date	Description
13 September, 2012	Added supported versions of Microsoft Active Directory. See "Third-party software requirements and recommendations" on page 31.

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 Standard depend on:

- The type and amount of information you want to protect
- The size of your organization
- The number of servers you want to manage

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 11.
- The system requirements for your Symantec Data Loss Prevention Standard installation

See "The effect of scale on system requirements" on page 12.

About installation tiers

Symantec Data Loss Prevention Standard supports three different installation types: single-tier, two-tier, and three-tier. A single-tier installation has the smallest hardware requirements and offers the simplest installation and management procedures. You can add additional Endpoint Prevent detection servers to a single-tier installation if you need to support additional endpoint computers at a later time. A single-tier installation is the most common deployment model for Symantec Data Loss Prevention Standard and is supported for large and small enterprise deployments.

Single-tier	To implement the single-tier installation, you install the database, the Enforce Server, and a detection server all on the same computer. You can add additional Endpoint Prevent detection servers to a single-tier installation if you need to support additional endpoint computers at a later time. See "Single-tier server minimum requirements for Symantec Data Loss Prevention Standard" on page 12.
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. See "Minimum system requirements for two-tier and three-tier deployments" on page 14.

Three-tier	To implement the three-tier installation, you install the Oracle database, the Enforce Server, and a detection server on separate computers. 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 two-tier and three-tier deployments" on page 14.

The effect of scale on system requirements

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

The key consideration in determining the deployment size for Symantec Data Loss Prevention Standard is the number of endpoint computers that you want to monitor. To simplify deployment and reduce hardware requirements, Symantec Data Loss Prevention Standard supports two single-tier hardware configurations to support up to 20,000 endpoint computers (for a small/medium enterprise) or over 20,000 endpoint computers (for a large enterprise).

See "Single-tier server minimum requirements for Symantec Data Loss Prevention Standard" on page 12.

If you choose to deploy a two-tier or three-tier installation, or you want to add an additional Endpoint Prevent detection server to a single-tier installation, the server requirements differ based on the component you are installing on the server computer.

See "Minimum system requirements for two-tier and three-tier deployments" on page 14.

See "Oracle database requirements" on page 23.

See "Operating system requirements for endpoint systems" on page 18.

Single-tier server minimum requirements for Symantec Data Loss Prevention Standard

Symantec Data Loss Prevention Standard is most commonly deployed in a single-tier configuration where the Oracle database, Enforce Server, and Endpoint Prevent detection server component reside on the same server computer. This

simplifies installation and administration, and has the fewest overall hardware requirements.

To support up to 20,000 endpoint computers in a single-tier configuration, the server must meet the small/medium enterprise server hardware requirements. See Table 1-2.

To support more than 20,000 endpoint computers in a single-tier deployment, use the large enterprise server hardware requirements. See Table 1-3.

Table 1-2 Single-tier server minimum requirements for a small/medium enterprise

Component	Description
Processor	2 x Intel Xeon E7420 (quad-core 2.14 Ghz) or equivalent
Memory	8 GB RAM
Storage	1 TB
Network	1 copper or fiber 1 Gb/100 Mb Ethernet NIC
Operating System	See "Operating system requirements for servers" on page 16.

Table 1-3 Single-tier server minimum requirements for a large enterprise

Component	Description
Processor	4 x Intel Xeon E7440 (quad-core 2.40 Ghz) or equivalent
Memory	16 GB RAM
Storage	2 TB
Network	1 copper or fiber 1 Gb/100 Mb Ethernet NIC
Operating System	See "Operating system requirements for servers" on page 16.

For very large enterprises, you may need to deploy an additional, dedicated Endpoint Prevent detection server to your single-tier installation. Or, you may choose to deploy a two-tier or three-tier installation instead of a single-tier deployment for flexibility in scaling your system. In either case, use the multi-tier server hardware requirements for the additional servers.

See "Minimum system requirements for two-tier and three-tier deployments" on page 14.

Minimum system requirements for two-tier and three-tier deployments

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

- See "Two-tier and three-tier minimum server requirements for a small/medium enterprise" on page 14.
- See "Two-tier and three-tier server minimum requirements for a large/very large enterprise" on page 15.
- See "Operating system requirements for servers" on page 16.

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

If you are upgrading an earlier version of Symantec Data Loss Prevention Standard to version 11, you can continue to use your existing Oracle10g database. After upgrading to Symantec Data Loss Prevention Standard 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 23.

Two-tier and three-tier minimum server requirements for a small/medium enterprise

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

Table 1-4 Two-tier and three-tier server minimum requirements for a small/medium enterprise

Required for	Enforce Server	Endpoint Prevent detection server
Processor	2 x 3.0 GHz CPU	2 x 3.0 GHz CPU

Table 1-4 Two-tier and three-tier server minimum requirements for a small/medium enterprise *(continued)*

Required for	Enforce Server	Endpoint Prevent detection server
Memory	6–8 GB RAM Two-tier deployments require additional memory for running Oracle.	6–8 GB RAM
Disk Requirements	500 GB, RAID 1+0 or RAID 5 configuration is recommended	140 GB
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 NIC

See "The effect of scale on system requirements" on page 12.

Two-tier and three-tier server minimum requirements for a large/very large enterprise

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

Table 1-5 Two-tier and three-tier server minimum requirements for a large/very large enterprise

Required For	Enforce Server	Endpoint Prevent detection server
Processor	2 x 3.0 GHz Dual Core CPU	2 x 3.0 GHz Dual Core CPU
Memory	8–16 GB RAM Two-tier deployments require additional memory for running Oracle.	8–16 GB RAM
Disk Requirements	1 TB, RAID 1+0 or RAID 5 configuration is recommended	140 GB
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 NIC

See "The effect of scale on system requirements" on page 12.

Operating system requirements for servers

Symantec Data Loss Prevention Standard 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 Standard 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 Standard. 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 Standard servers and endpoint computers. Localized versions of Linux platforms are supported only for Symantec Data Loss Prevention Standard servers.

See "Supported languages for detection" on page 20.

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

See "Minimum system requirements for two-tier and three-tier deployments" on page 14.

Linux partition guidelines

Minimum free space requirements for Linux partitions vary according to the specific details of your Symantec Data Loss Prevention Standard 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 1-7 on page 18.

Table 1-6 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.
`/opt`	500 GB for Small/Medium installations 1 TB for Large/Very Large installations	Contains installed programs such as Symantec Data Loss Prevention Standard, 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 log files.
`/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 1-7 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 Standard and the Oracle client.
`/var`	15 GB for Small/Medium installations 46 GB for Large/Very Large installations	Contains log files.
`/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.

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 18.
- See "Memory and disk space requirements for the Symantec DLP Agent" on page 19.
- See "Symantec DLP Agent connectivity requirements" on page 19.

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 20.

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

See "About Endpoint Data Loss Prevention compatibility" on page 33.

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 Standard System Adminitration Guide* for information about configuring Endpoint Server redundancy.

Supported languages for detection

Symantec Data Loss Prevention Standard 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.

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

Table 1-8 Languages supported by Symantec Data Loss Prevention Standard

Language	Version 10.5	Versions 11.0, 11.1.x, 11.5, 11.6
Arabic	Yes	Yes
Brazilian Portuguese	Yes	Yes
Chinese (traditional)	Yes	Yes
Chinese (simplified)	Yes	Yes
Czech	Yes	Yes
Danish	Yes	Yes
Dutch	Yes	Yes
English	Yes	Yes
Finnish	Yes	Yes
French	Yes	Yes
German	Yes	Yes
Greek	Yes	Yes
Hebrew	Yes	Yes
Hungarian	Yes	Yes
Italian	Yes	Yes

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

Language	Version 10.5	Versions 11.0, 11.1.x, 11.5, 11.6
Japanese	Yes	Yes
Korean	Yes	Yes
Norwegian	Yes	Yes
Polish	Yes	Yes
Portuguese	Yes	Yes
Romanian	Yes	Yes
Russian	Yes	Yes
Spanish	Yes	Yes
Swedish	Yes	Yes
Turkish	Yes*	Yes*

*Symantec Data Loss Prevention Standard 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 Standard 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 Standard 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. 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 Standard 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 Standard documentation.

As they become available, language packs for Symantec Data Loss Prevention Standard 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
Russian	RU_RU

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

Oracle database requirements

All new Symantec Data Loss Prevention Standard 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 Standard includes Oracle 11g and the necessary patches.

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

If you are upgrading an earlier version of Symantec Data Loss Prevention Standard 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 Standard 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 Standard 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 "Two-tier and three-tier minimum server requirements for a small/medium enterprise" on page 14.
  See "Two-tier and three-tier server minimum requirements for a large/very large enterprise" on page 15.

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

- 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 Standard. 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 Standard 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

See the *Symantec Data Loss Prevention Standard 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 Standard 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 Standard can operate with an RFC 2560-compliant OCSP responder. If the OCSP responder cannot be reached, Symantec Data Loss Prevention Standard 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 Standard extracts the HTTP URL from the CRL distribution point extension to the X.509 certificate. Note, however, that Symantec Data Loss Prevention Standard 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 Standard System Administration Guide*.

Virtual server and virtual workstation support

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 Standard 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 27.

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).

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

See "Minimum system requirements for two-tier and three-tier deployments" on page 14.

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.

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 Standard 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 30. ■ 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 Standard 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 Standard 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.
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 26.	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 Standard 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.

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 Standard deployment.

Table 1-13 Recommended third-party software

Software	Location	Description
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:

- Symantec Veritas Cluster Server compatibility
- About Endpoint Data Loss Prevention compatibility

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 Standard Enforce Server and Oracle database hosts.

Table 2-1 describes Data Loss Prevention and VCS compatibility according to operating system platform.

Table 2-1 Data Loss Prevention and VCS compatibility

Operating system	Symantec Data Loss Prevention Standard 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

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 34.

See "Endpoint Prevent supported applications" on page 35.

Endpoint Data Loss Prevention supported operating systems

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

Table 2-2 Endpoint Data Loss Prevention supported operating systems

Operating system	Version	Symantec Data Loss Prevention Standard			
		Version 10.0 (Does not apply to Symantec Data Loss Prevention Standard Standard)	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)

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

Operating system	Version	Symantec Data Loss Prevention Standard			
		Version 10.0 (Does not apply to Symantec Data Loss Prevention Standard Standard)	Version 10.5	Version 11.0	Versions 11.1x, 11.5, and 11.6
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 Standard System Administration Guide* for more information about configuring and using application monitoring.

Table 2-3 Applications supported by Endpoint Prevent

Feature	Software	Version	Symantec Data Loss Prevention Standard	
			Version 10.5	Versions 11.x
HTTP	All	All	Yes	Yes
Secure HTTP (HTTPS)	Internet Explorer	6.0	Yes	Yes

Table 2-3 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention Standard	
			Version 10.5	Versions 11.x
		7.0	Yes	Yes
		8.0	Yes	Yes
		9.0	No	Yes (11.1.1 and later)
	Firefox	2.0	Yes	Yes
		3.0	Yes	Yes
		3.5	Yes	Yes
		3.6	Yes	Yes
		4.0	No	Yes (11.1.1 and later)
Instant messaging	Yahoo Messenger	7.5	Yes	Yes
		8.0	Yes	Yes
		8.1	Yes	Yes
		9.0	Yes	Yes
		10.0	Yes	Yes
	MSN Messenger	8.1	Yes	Yes
		9.0	Yes	Yes
	AIM	5.9	Yes	Yes
		6.0	Yes	Yes
		6.1	Yes	Yes
		6.5	Yes	Yes
		6.8	Yes	Yes
		6.9	Yes	Yes
	AIM Pro	1.4	Yes	Yes

Table 2-3 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention Standard	
			Version 10.5	Versions 11.x
		1.5	Yes	Yes
Email	Outlook	2002	Yes	Yes
		2003	Yes	Yes
		2007	Yes	Yes
		2010 (32-bit and 64-bit)	No	Yes
	Eudora		No	No
	Thunderbird		No	No
	Lotus Notes	6.5	Yes	Yes
		7.0	Yes	Yes
		7.0.2 Multiuser	Yes	Yes
		8.0	Yes	Yes
		8.5	Yes	Yes
		8.5.1		Yes (11.1.1 and later)
		8.5.3		Yes (11.1.1 and later)
FTP			Yes	Yes
CD/DVD	BsClip		Yes	Yes
	Bs Recorder Gold		Yes	Yes
	BurnAware		Yes	Yes
	Cheetah Burner		Yes	Yes
	Command Burner		Yes	Yes

Table 2-3 Applications supported by Endpoint Prevent *(continued)*

Feature	Software	Version	Symantec Data Loss Prevention Standard	
			Version 10.5	Versions 11.x
	CopyToDVD		Yes	Yes
	Creator10		Yes	Yes
	Deep Burner (32-bit Windows XP)		Yes	Yes
	GEAR for Windows		Yes	Yes
	mkisofs		Yes	Yes
	Nero		Yes	Yes
	NeroStartSmart		Yes	Yes
	Roxio		Yes	Yes
	Roxio RecordNow		Yes	Yes
	Roxio5		Yes	Yes
	Roxio Mediahub		Yes	Yes
	Silent Night Micro Burner		Yes	Yes
	Star Burn		Yes	Yes
	Windows native CD/DVD writer			Yes

Chapter 3

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 interoperates with many other applications.

See "Operating system requirements for endpoint systems" on page 18.

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 40.
- Client-side

See "Symantec DLP Agent and client-side application configuration" on page 47.

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 40.
- McAfee ePolicy Orchestrator 4.0
  See "Configuring McAfee ePolicy Orchestrator to work with Symantec DLP Agent (server-side)" on page 41.
- McAfee Total Protection Service
  See "Configuring McAfee Total Protection Service to work with Symantec DLP Agent (server-side)" on page 42.
- Sophos Enterprise Console
  See "About Sophos Enterprise Console and Symantec DLP Agent" on page 43.
- Symantec Critical System Protection
  See "Configuring Symantec Critical System Protection to work with Symantec DLP Agent (server-side)" on page 45.

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 50.

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 43.
- Sophos Firewall systems
  See "Configuring Sophos Firewall to work with Symantec DLP Agent (server-side)" on page 44.
- Sophos Application Control
  See "Configuring Sophos Application Control to work with Symantec DLP Agent (server-side)" on page 44.

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 43.

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 43.

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 48.
- Symantec AntiVirus 9.0
  See "Configuring Symantec AntiVirus 9.0 to work with Symantec DLP Agent (client-side)" on page 47.
- 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 48.
- 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 49.
- McAfee Total Protection Service Firewall
  See "Configuring McAfee Total Protection Service Firewall to work with Symantec DLP Agent (client-side)" on page 50.
- McAfee VirusScan
  See "Configuring McAfee VirusScan to work with Symantec DLP Agent (client-side)" on page 50.

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 42.

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.

Index

A

Adobe Reader 31
AIM 36
AIM Pro 36
Apache Tomcat 31

B

boot filesystem 24
browser requirements 25
Bs Recorder Gold 37
BsClip 37
BurnAware 37

C

CD/DVD copying 37
Cheetah Burner 37
Cisco CSA Management Center 40
Command Burner 37
communications requirements
    large/very large installations 15
CopyToDVD 38
Creator10 38

D

Deep Burner 38

E

email applications 37
Endpoint Data Loss Prevention compatibility 33
    operating systems 34
Endpoint Prevent supported applications 35
Eudora 37

F

Firefox 25
FTP 37

G

GEAR for Windows 38

I

installation 11
    See also detection server installation
    See also Enforce server installation
    See also single-tier installation
    See also three-tier installation
    See also two-tier installation
installation scale 12
installations
    size of 12
Instant messaging 36
Internet Explorer 25

J

Java Runtime Environment (JRE) 31

L

large/very large installations
    communications requirements 15
    disk requirements 15
    hardware requirements 15
    memory requirements 15
    processor requirements 15
LDAP browser 32
Linux platforms
    browsers, supported 25
    operating system requirements 16
    RPMs, required 32
    SeLinux 32
Lotus Notes 37

M

McAfee ePolicy Orchestrator 41
McAfee Total Protection Service 42, 50
McAfee VirusScan Console 50
Microsoft Internet Explorer 25
mkisofs 38
Mozilla Firefox 25
MSN Messenger 36

N

Nero 38

O

operating systems
    endpoint system requirements 18
    server requirements 16
opt filesystem 24
Oracle database requirements 23
Outlook 37

P

planning considerations 11
product compatibility
    Endpoint Data Loss Prevention 33
    Endpoint operating systems 34
    Endpoint Prevent supported applications 35

R

Red Hat Package Managers 32
requirements. *See* system requirements
Roxio 38
RPMs 32

S

SeLinux 32
Silent Night Micro Burner 38
single-tier installation 11
small/medium installations
    communications requirements 15
    disk requirements 15
    hardware requirements 14
    memory requirements 15
    processor requirements 14
software, third-party
    recommended 32
    required 31
Sophos Anti-virus 43, 49
Sophos Application Control 44
Sophos Enterprise Console 43
Sophos Firewall 44
Star Burn 38
Symantec AntiVirus 9.0 47
Symantec Critical System Protection 45
Symantec DLP Agent
    Cisco CSA Management Center 40
    client-side applications 47
Symantec DLP Agent *(continued)*
    McAfee ePolicy Orchestrator 41
    McAfee Total Protection Service 42, 50
    McAfee VirusScan Console 50
    server-side application 40
    Sophos Anti-virus 43, 49
    Sophos Application Control 44
    Sophos Enterprise Console 43
    Sophos Firewall 44
    Symantec AntiVirus 9.0 47
    Symantec Critical System Protection 45
    Symantec NetBackup 51
    Trend Micro PC-cillin 48
Symantec NetBackup and Windows Vista 51
Sysinternals Suite 32
system requirements
    browser requirements 25
    large/very large installations 15
    operating systems, endpoints 18
    operating systems, servers 16
    Oracle database requirements 23
    planning considerations 11
    scale of installation 12
    small/medium installations 14
    software, third-party (recommended) 32
    software, third-party (required) 31
    virtualization support 26

T

three-tier installation 11
Thunderbird 37
tiers, installation 11
Tomcat 31
Trend Micro PC-cillin 48
two-tier installation 11

V

virtualization support 26
VM. *See* virtualization support
VMware 31

W

Windows 2003 34
Windows 2008 64-bit 35
Windows 7 34
Windows platforms
    browsers, supported 25
    enpoint operating systems 18

Windows platforms *(continued)*
operating system requirements 16
Windows Vista 34
Windows Vista and Symantec NetBackup 51
Windows XP 34

Y

Yahoo Messenger 36