# Symantec™ Data Loss Prevention System Requirements and Compatibility Guide

Version 12.5.x

Last updated: 6 January 2015

# Symantec Data Loss Prevention System Requirements and Compatibility Guide

Documentation version: 12.5f

Last updated: 6 January 2015

## 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 software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

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

## Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

## Licensing and registration

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

www.symantec.com/business/support/

## Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

## Support agreement resources

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

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

# Contents

Chapter 1

# About this guide

This chapter includes the following topics:



## About updates to Symantec Data Loss Prevention system requirements

System requirements as described in this guide are occasionally updated as new information becomes available. You can find the latest version of the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* at the following link to the Symantec Data Loss Prevention knowledgebase.

https://www.symantec.com/docs/TECH221192

The following table provides the history of updates to this version of the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.

**Table 1-1** Change history for the System Requirements and Compatibility Guide

| Date | Description |
|---|---|
| 6 January 2015 | Corrected browser support for Enforce Server administration console access. |
| 19 December 2014 | Added support for Network Discover scanning of Oracle Database 12c (12.1.0.2). |

**Table 1-1** Change history for the System Requirements and Compatibility Guide *(continued)*

| Date | Description |
|---|---|
| 5 December 2014 | Added support for Network Discover scanning of Oracle Database 11g (11.2.0.4). Added DLP Agent support for Apple Mac OS X 10.10. Added support for running Mac DLP Agents on VMware Fusion. Added support for Symantec Data Loss Prevention installations on Microsoft Windows Server 2012 R2 and Red Hat Enterprise Linux 5.11. Added DLP Agent support for Microsoft Windows Server 2012 R2. Added Endpoint Prevent support for Microsoft Internet Explorer 11. |
| 13 November 2014 | Added support for Microsoft SQL Server 2014. Added support for IBM Notes 9.0.x. |
| 1 October 2014 | Added support for Microsoft Active Directory 2012. Added support for Single Server Installations on Red Hat Enterprise Linux 6.5 (64-bit). |
| 29 September 2014 | Added Discover target support for Microsoft Office SharePoint Server 2013 SP1 on Microsoft Windows Server 2012 R2. Added support for Firefox version 32. Added support for Microsoft Windows 8.1 Update 2 Enterprise 64-bit operating system. |
| 22 August 2014 | Added support for Firefox version 30. |
| 19 August 2014 | Added Discover target support for Microsoft SQL Server 2008 R2 and 2012. Added support for Napatech driver version 4.26c. |
| 14 August 2014 | Added support for Single Server installations on Microsoft Windows Server 2012. Added support for Firefox version 31. |
| 17 July 2014 | Corrected supported Squid proxy version. Clarified Secure ICAP support. Corrected supported versions of Windows Server 2012. |
| 17 June 2014 | Added support for Firefox versions 28 and 29. |

Chapter 2

# 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 12.
- The system requirements for your Symantec Data Loss Prevention installation

See "The effect of scale on system requirements" on page 13.

## 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 for branch offices, small organizations, or for testing purposes.

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

See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 14.

## 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 three sample deployments based on enterprise size. Review these sample deployments to understand which best matches your organization's environment.

**Table 2-1** Types of enterprise deployments

| Variable | Small Organization | Small/Medium Enterprise | Large/Very Large Enterprise |
|---|---|---|---|
| Number of employees | < 1000 | < 10,000 | > 10,000 |
| Volume of network traffic to monitor | 30-40 Mbps | 30-40 Mbps | > 40 Mbps |

**Table 2-1** Types of enterprise deployments *(continued)*

| Variable | Small Organization | Small/Medium Enterprise | Large/Very Large Enterprise |
|---|---|---|---|
| EDM/IDM size | EDM 4 million cells or IDM 250 MB (1400 files). See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing for enterprise deployments. | See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing for enterprise deployments. | See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing for enterprise deployments. |
| Hardware requirements | See "Small organization minimum hardware requirements" on page 15. | See "Small/medium enterprise minimum hardware requirements" on page 15. | See "Large/very large enterprise minimum hardware requirements" on page 16. |

For additional related information see also *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines*, available at the Symantec Data Loss Prevention knowledgebase at http://www.symantec.com/docs/TECH221999.

# Minimum system requirements for Symantec Data Loss Prevention servers

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

- See "Small organization minimum hardware requirements" on page 15.
- See "Small/medium enterprise minimum hardware requirements" on page 15.
- See "Large/very large enterprise minimum hardware requirements" on page 16.
- See "Operating system requirements for servers" on page 18.

New installations of Symantec Data Loss Prevention version 12.5 require Oracle 11.2.0.3 or 11.2.0.4 to store the Enforce Server database, depending on your operating system.

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

See "Oracle database requirements" on page 26.

## Small organization minimum hardware requirements

The following table provides the system requirements for branch office or small organization single-tier systems.

**Table 2-2**

| Required for | Single Server Installation |
|---|---|
| Processor | 2 x 2.2 GHz 8-core CPU |
| Memory | 64 GB RAM |
| Disk | 3 TB, RAID 5 configuration (with a minimum of five spindles) |
| NICs | 1 copper or fiber 1 Gb Ethernet NIC (if you are using Network Monitor you will need a minimum of two NICs) |

## Small/medium enterprise minimum hardware requirements

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

**Table 2-3** Small/medium enterprise minimum system requirements

| Required for | Enforce Server | Network Monitor | Network Discover, Network Prevent, Mobile Email Monitor, Mobile Prevent, Endpoint Prevent, or Classification server |
|---|---|---|---|
| Processor | 2 x 3.0 GHz CPU | 2 x 3.0 GHz CPU | 2 x 3.0 GHz CPU |
| Memory | 6–8 GB RAM (EDM/IDM size can increase memory requirements)<br>Two-tier deployments may require additional memory for running Oracle. | 6–8 GB RAM (EDM/IDM size can increase memory requirements. See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing.) | 6–8 GB RAM (EDM/IDM size can increase memory requirements. See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing.) |

**Table 2-3** Small/medium enterprise minimum system requirements *(continued)*

| Required for | Enforce Server | Network Monitor | Network Discover, Network Prevent, Mobile Email Monitor, Mobile Prevent, Endpoint Prevent, or Classification server |
|---|---|---|---|
| Disk | 500 GB, RAID 1+0 or RAID 5 configuration is recommended. RAID 5 is not recommended for computers that host the Oracle database.<br>For Network Discover deployments, approximately 150 MB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target. | 140 GB | 140 GB<br>For Network Discover deployments, approximately 150 MB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target. |
| NICs | 1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with detection servers. | 1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with the Enforce Server. | 1 copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with the Enforce Server. |

See "Oracle database requirements" on page 26.

See "The effect of scale on system requirements" on page 13.

## Large/very large enterprise minimum hardware requirements

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

**Table 2-4** Large/Very Large enterprise minimum system requirements

| Required For | Enforce Server | Network Monitor | Network Discover, Network Prevent, Mobile Email Monitor, Mobile Prevent, Endpoint Prevent, or Classification Server |
|---|---|---|---|
| Processor | 2 x 3.0 GHz Dual Core CPU | 2 x 3.0 GHz Dual Core CPU | 2 x 3.0 GHz Dual Core CPU |
| Memory | 8–16 GB RAM (EDM/IDM size can increase memory requirements)<br>Two-tier deployments require additional memory for running Oracle. | 8–16 GB RAM (EDM/IDM size can increase memory requirements) | 8–16 GB RAM (EDM/IDM size can increase memory requirements) |
| Disk Requirements | 1 TB, RAID 1+0 or RAID 5 configuration is recommended. RAID 5 is not recommended for computers that host the Oracle database.<br>For Network Discover deployments, approximately 1 GB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target. | 140 GB | 140 GB<br>For Network Discover deployments, approximately 1 GB of disk space is required to maintain incremental scan indexes. This is based on an overhead of 5 MB per incremental scan target and 50 bytes per item in the target. |
| NICs | To communicate with detection servers:<br>1 copper or fiber 1 Gb/100 Mb Ethernet NIC | To communicate with the Enforce Server:<br>1 copper or fiber 1 Gb/100 Mb Ethernet<br>For network traffic monitoring (pick one):<br>1 copper or fiber 1 Gb/100 Mb Ethernet NIC. | To communicate with the Enforce Server:<br>1 copper or fiber 1 Gb/100 Mb Ethernet NIC |
| High-speed packet capture cards | n/a | See "High-speed packet capture cards" on page 42. | n/a |

See "Oracle database requirements" on page 26.

See "The effect of scale on system requirements" on page 13.

# Operating system requirements for servers

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

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

- Microsoft Windows Server 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)
- Microsoft Windows Server 2012, Datacenter Edition (64-bit)
- Microsoft Windows Server 2012, Standard Edition (64-bit)
- Microsoft Windows Server 2012 R2, Datacenter Edition (64-bit)
- Microsoft Windows Server 2012 R2, Standard Edition (64-bit)
- Red Hat Enterprise Linux 5.7 through 5.11 (64-bit)
- Red Hat Enterprise Linux 6.4 and 6.5 (64-bit)

## Operating system requirements for Single Server installations

Symantec Data Loss Prevention supports the following operating systems for Single Server installations:

- 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)
- Microsoft Windows Server 2012, Datacenter Edition (64-bit)
- Microsoft Windows Server 2012, Standard Edition (64-bit)
- Microsoft Windows Server 2012 R2, Datacenter Edition (64-bit)
- Microsoft Windows Server 2012 R2, Standard Edition (64-bit)

- Red Hat Enterprise Linux 6.5 (64-bit)

English language as well as localized versions of both Linux and Windows operating systems are supported.

See "Supported languages for detection" on page 23.

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

## Linux partition guidelines

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

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

See Table 2-6 on page 20.

**Table 2-5** Linux partition minimum size guidelines—Enforce Server with Oracle database

| Partition | Minimum free space | Description and comments |
|---|---|---|
| `/home` | 6 GB | Store the Oracle installation tools, Oracle installation ZIP files, and Oracle critical patch update (CPU) files in `/home`. |
| `/tmp` | 1.2 GB | The Oracle installer and installation tools require space in this directory. |
| `/opt` | 500 GB for Small/Medium installations<br>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 2-5** Linux partition minimum size guidelines—Enforce Server with Oracle database *(continued)*

| Partition | Minimum free space | Description and comments |
|---|---|---|
| `/var` | 15 GB for Small/Medium installations<br>46 GB for Large/Very Large installations | Contains logs, EDM/IDM indexes, incremental scan indexes, and network packet capture directories.<br>**Note:** The `/var/spool/pcap` and `/var/SymantecDLP/drop_pcap` directories must reside on the same partition or mount point. |
| `/boot` | 100 MB | This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported). |
| swap | Equal to RAM | If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts. |

**Table 2-6** Linux partition minimum size guidelines—Enforce Server without a database, or detection server

| Partition | Minimum size guidelines | Description and comments |
|---|---|---|
| `/opt` | 10 GB | Contains installed programs such as Symantec Data Loss Prevention and the Oracle client. |
| `/var` | 15 GB for Small/Medium installations<br>46 GB for Large/Very Large installations | Contains logs, EDM/IDM indexes, incremental scan indexes, and network packet capture directories.<br>**Note:** The `/var/spool/pcap` and `/var/SymantecDLP/drop_pcap` directories must reside on the same partition or mount point. |
| `/boot` | 100 MB | This must be in its own ext2 or ext3 partition, not part of soft RAID (hardware RAID is supported). |
| swap | Equal to RAM | If you need to have the memory dump in case of system crash (for debugging), you may want to increase these amounts. |

# Endpoint computer requirements for the Symantec DLP Agent

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

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

## 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 SP2 (32-bit), or Windows Server 2003 R2 (32-bit)
- Microsoft Windows Server 2008 Enterprise or Standard Editions R2 (64-bit)
- Microsoft Windows Server 2012 R2 Datacenter, Standard, Essential, or Foundation Editions (64-bit, Desktop mode only)
- Microsoft Windows 7 Enterprise, Professional, or Ultimate, including Service Pack 1 (32-bit or 64-bit)
- Microsoft Windows 8 Enterprise 64-bit PC operating system

  **Note:** Windows Store (Metro UI) apps are not supported.

- Microsoft Windows 8.1 Enterprise 64-bit PC operating system
- Microsoft Windows 8.1 Update 1 Enterprise 64-bit PC operating system
- Microsoft Windows 8.1 Update 2 Enterprise 64-bit PC operating system

  **Note:** Windows Store (Metro UI) apps are not supported.

- Apple Mac OS X 10.8 (64-bit)
- Apple Mac OS X 10.9 (64-bit)
- Apple Mac OS X 10.10 (64-bit)

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

See "Supported languages for detection" on page 23.

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

See "About Endpoint Data Loss Prevention compatibility" on page 50.

## 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 Data Loss Prevention for Mobile requirements

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

**Note:** The Symantec Data Loss Prevention Mobile Prevent for Web detection server is not supported in a virtual or hosted environment, or on Single Server installations.

For system requirements for Mobile Prevent detection servers:

- See "Small/medium enterprise minimum hardware requirements" on page 15.
- See "Large/very large enterprise minimum hardware requirements" on page 16.

**Table 2-7** Mobile Prevent requirements

| Requirement | Description |
|---|---|
| Supported devices | iPad 2, iPad 3, iPad Mini<br>iPhone 4, iPhone 4S, iPhone 5, iPhone 5S, iPhone 5C (all carriers) |
| Operating systems | iOS for iPad: 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3, 7<br>iOS for iPhone: 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3, 7 |
| ActiveSync | (Required only for detection of corporate email) Microsoft Exchange 2003, 2007, and 2010 with ActiveSync |
| Web proxy | Blue Coat Proxy SG version 5.5.3.1, 6.2.12.1, and 6.5.x for Mobile Prevent, or for Mobile Prevent deployed with Network Prevent for Web<br>**Note:** Your proxy server must not use network address translation (NAT) where it is located in your infrastructure. |
| VPN server | Cisco ASA series<br>Cisco AnyConnect<br>Juniper SA series |

# Supported languages for detection

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

**Table 2-8** Languages supported by Symantec Data Loss Prevention

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

**Table 2-8** Languages supported by Symantec Data Loss Prevention *(continued)*

| Language | Version 10.x | Versions 11.0, 11.1.x, 11.5, 11.6 | Version 12.x |
|---|---|---|---|
| English | Yes | Yes | Yes |
| Finnish | Yes | Yes | Yes |
| French | Yes | Yes | Yes |
| German | Yes | Yes | Yes |
| Greek | Yes | Yes | Yes |
| Hebrew | Yes | Yes | Yes |
| Hungarian | Yes | Yes | Yes |
| Italian | Yes | Yes | Yes |
| Japanese | Yes | Yes | Yes |
| Korean | Yes | Yes | Yes |
| Norwegian | Yes | Yes | Yes |
| Polish | Yes | Yes | Yes |
| Portuguese | Yes | Yes | Yes |
| Romanian | Yes | Yes | Yes |
| Russian | Yes | Yes | Yes |
| Spanish | Yes | Yes | Yes |
| Swedish | Yes | Yes | Yes |
| Turkish | Yes* | Yes* | Yes* |

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

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

A number of capabilities are not implied by this support:

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

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

# Available language packs

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

also contain translated versions of selected Symantec Data Loss Prevention documentation.

As they become available, language packs for Symantec Data Loss Prevention are distributed along with the software products they support. You can also download and add a language pack to an installation. Language packs do not require any additional purchase or license. Consult the *Symantec Data Loss Prevention Administration Guide* for details on how to add and enable a language pack. Language packs are distributed in the `Symantec_DLP_12.5_Lang_Pack-ML.zip` file on the Symantec FileConnect website. When you extract the contents of the ZIP file, the individual language pack files have names in the form:

`Symantec_DLP_12.5_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 installations must install and use Oracle 11g Standard Edition version 11.2.0.3 or 11.2.0.4 (64-bit) with the most recent Critical Patch Update. Symantec Data Loss Prevention includes Oracle 11g and the necessary patches.

**Note:** Symantec only supports the Standard Edition of the Oracle database, but the Symantec Data Loss Prevention database schema is supported on all editions of Oracle.

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

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

- Three-tier deployment.
  System requirements for a dedicated Oracle server are listed below. Note that dedicated Oracle server deployments also require that you install the Oracle 11g Client on the Enforce Server computer to communicate with the remote Oracle 11g instance.
- Single- 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 organization minimum hardware requirements" on page 15.
  See "Small/medium enterprise minimum hardware requirements" on page 15.
  See "Large/very large enterprise minimum hardware requirements" on page 16.

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

- One of the following operating systems:
  - Microsoft Windows Server 2008 R2 Standard or Enterprise (64-bit) (Oracle 11.2.0.3)
  - Microsoft Windows Server 2008 R2 SP1 Standard or Enterprise (64-bit) (Oracle 11.2.0.3)
  - Microsoft Windows Server 2012 Standard or Datacenter (64-bit) (Oracle 11.2.0.4)
  - Red Hat Enterprise Linux 5.7 through 5.10 (64-bit) (Oracle 11.2.0.3)
  - Red Hat Enterprise Linux 6.4 or 6.5 (64-bit) (Oracle 11.2.0.4)
- 6 GB of RAM
- 6 GB of swap space (equal to RAM up to 16 GB)
- 500 GB – 1 TB of disk space for the Enforce database

**Note:** Support for 32-bit platforms for Oracle is discontinued as of version 12.0 of Symantec Data Loss Prevention.

See the *Symantec Data Loss Prevention 64-bit Server Migration and Tuning Guide* for more information.

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

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

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

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

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

# Browser requirements for accessing the Enforce Server administration console

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

- Microsoft Internet Explorer 9.x or 10
- Mozilla Firefox 24 or 27

Adobe Flash Player 11.1 is required to view the folder risk report for Network Discover (**Incidents > Discover > Folder Risk Report**).

# 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 accesses the Enforce Server administration console URL. The client certificate must contain a unique CN value that maps to an active user account in the Enforce Server configuration.

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

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

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

# Virtual server and virtual workstation support

Symantec supports running Symantec Data Loss Prevention on VMware ESX 4.x and later virtualization products, provided that the virtualization environment is running a supported operating sytem.

See “Operating system requirements for servers” on page 18.

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

See "Minimum system requirements for Symantec Data Loss Prevention servers" on page 14.

Be aware of the following limitations for virtualization:

- Endpoint Prevent servers are supported only for configurations that do not exceed the recommended number of connected agents.
- 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.
- Symantec does not support running the Network Monitor or Mobile Prevent for Web detection servers on virtual machines.
- Symantec Data Loss Prevention does not support Single Server installations on virtual machines.

Note that a variety of factors influence performance of virtual machine configurations, including the number of CPUs, the amount of dedicated RAM, and the resource reservations for CPU cycles and RAM. The virtualization overhead and guest operating system overhead can lead to a performance degradation in throughput for large datasets compared to a system running on physical hardware. Use your own test results as a basis for sizing deployments to virtual machines.

See the *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines*, available at the Symantec Data Loss Prevention knowledgebase at http://www.symantec.com/docs/TECH221999, for additional information about running Network Prevent servers on virtual machines.

# Virtual desktop and virtual application support with Endpoint Prevent

You can deploy the DLP Agent on Citrix and VMware virtual machines.

## Citrix virtualization support

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

are protected by the agent monitor need to have a valid Endpoint Prevent license. The license is required whether a Symantec DLP Agent is installed on the client or not.

---

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

---

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

**Table 2-9** Citrix virtualization support and limitations

| Supported Citrix products | Limitations |
| --- | --- |
| ■ Citrix XenApp 4.5 on Windows Server 2003 (32-bit) Enterprise Edition SP2<br>■ Citrix XenApp 6 on Windows Server 2008 Enterprise Edition R2 (64-bit)<br>■ Citrix XenApp 6.5 on Windows Server 2008 Enterprise Edition R2 (64-bit) | |

**Table 2-9** Citrix virtualization support and limitations *(continued)*

| Supported Citrix products | Limitations |
|---|---|
| | Performance and deployment:<br>■ You must install the Symantec DLP Agent software on each XenApp server host, and on any individual application servers that publish applications through XenApp.<br>■ All detection on Citrix XenApp is performed in a single thread (all user activities are analyzed sequentially).<br>■ 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.<br>■ 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.<br>See "" on page 35.<br>■ 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.<br>Endpoint Prevent features:<br>■ 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.<br>■ 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.<br>■ FTP events are not supported.<br>■ Printer/Fax events for files on endpoint-published drives are not monitored for Adobe Acrobat Reader.<br>■ Instant messenger events (MSN IM, Yahoo IM, and AIM) have not been tested and are not supported.<br>■ IP addresses in Data Loss Prevention incident snapshots contain the IP address of the XenApp server, and not a Citrix client.<br>■ If the Symantec DLP Agent software blocks an attempted copy to a client drive, it does not provide an option to restore or recover |

**Table 2-9** Citrix virtualization support and limitations *(continued)*

| Supported Citrix products | Limitations |
|---|---|
| | the file at a later time. |
| ■ Citrix XenDesktop 4 on Windows 7 (32-bit or 64-bit)<br>■ Citrix XenDesktop 5.0 on Windows 7 SP1 (32-bit or 64-bit)<br>■ Citrix XenDesktop 5.6 on Windows 7 SP1 (32-bit or 64-bit) | Performance and deployment:<br>■ You must install the Symantec DLP Agent software on each virtual machine on the XenDesktop server.<br>■ 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.<br>Endpoint Prevent features:<br>■ 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.<br>■ FTP events are not supported.<br>■ Printer/Fax events for files on endpoint-published drives are not monitored for Adobe Acrobat Reader.<br>■ Instant messenger events (MSN IM, Yahoo IM, and AIM) have not been tested and are not supported.<br>■ IP addresses in Data Loss Prevention incident snapshots contain the IP address of the XenDesktop virtual machine, and not a Citrix client.<br>■ 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.

### VMware virtualization support

Symantec supports running the Symantec DLP Agent software on virtual workstations using VMware Workstation 6.5.x, VMware View 4.6, VMware Fusion (Mac OS), and Hyper-V.

# Third-party software requirements and recommendations

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

- Table 2-10 for required software
- Table 2-11 for required Linux RPMs
- Table 2-12 for recommended software

**Table 2-10** Required third-party software

| Software | Required for | Description |
|---|---|---|
| Adobe Reader | All systems | Adobe Reader is required for reading the Symantec Data Loss Prevention documentation.<br>Download from Adobe. |
| Apache Tomcat version 7.0.52 | Enforce Server | Required to support the reporting system.<br>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) 1.7.0_51 | All servers | The Symantec DLP Installation Wizard automatically installs the correct JRE version. |
| Flex SDK 4.6 | Network Discover Server | Required SDK for Folder Risk Reporting. |

**Table 2-10** Required third-party software *(continued)*

| Software | Required for | Description |
|---|---|---|
| Napatech driver version 4.22a (RHEL 5.10 only), 4.22c (Windows Server 2008 R2 only), 4.26a and 4.26c (Linux and Windows) | Napatech NT4E high-speed packet capture card | Provides high-speed montitoring.<br>Napatech cards are not supported on Single Server installations. |
| WinPcap 4.1.1, 4.1.2, 4.1.3 | Required for Windows-based Network Monitor Server. WinPcap 4.1.3 is required for Microsoft Windows Server 2012.<br>Recommended for all Windows-based detection servers. | Windows packet capture library.<br>Download from winpcap.org. |
| Endace card driver 4.2.4 | Detection servers equipped with an Endace network measurement card. | Endace cards are not supported on Single Server installations.<br>Download from Endace.<br>See "Small/medium enterprise minimum hardware requirements" on page 15. |
| VMware | Required to run supported components in a virtualized environment.<br>See "Virtual server and virtual workstation support" on page 29. | Virtualization software.<br>Download from VMware. |
| Microsoft Active Directory 2003, 2008 R2, or 2012 | Required versions for connecting to Active Directory. | Provides directory services for Windows domain networks. |

In addition to the Linux Minimal Installation, Linux-based Symantec Data Loss Prevention servers require the Red Hat Package Managers (RPM) listed in Table 2-11.

**Table 2-11** Required Linux RPMs

| Linux-based servers | Required RPMs |
|---|---|
| Enforce Server<br>Oracle server | apr<br>apr-util<br>binutils<br>compat-libstdc++-296<br>compat-libstdc++-33<br>expat<br>libicu<br>Xorg-x11*<br><br>*Required only for graphical installation. Console-mode installation does not require an X server. |
| Network Monitor Server | apr<br>apr-util<br>compat-libstdc++-296<br>compat-libstdc++-33<br>expat<br>libicu<br>Xorg-X11*<br><br>*Required only for graphical installation. Console-mode installation does not require an X server. |

Red Hat Enterprise Linux versions 6.4 and 6.5 have these additional dependencies:

- compat-openldap
- compat-expat1
- compat-db43
- openssl098e

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

Symantec recommends the third-party software listed in Table 2-12 for help with configuring and troubleshooting your Symantec Data Loss Prevention deployment.

**Table 2-12** 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.<br>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.<br>Download the latest version from Microsoft. |
| LDAP browser | Enforce Server | An LDAP browser is recommended for configuring or troubleshooting Active Directory or LDAP. |

Chapter 3

# Product compatibility

This chapter includes the following topics:



## Environment compatibility and requirements for Network Prevent for Email

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

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

- The MTA or hosted email service must be capable of strict SMTP compliance. It must be able to send and receive mail using only the following command verbs: HELO (or EHLO), RCPT TO, MAIL FROM, QUIT, NOOP, and DATA.
- When running the Network Prevent for Email Server in reflecting mode, the upstream MTA must be able to route messages to the Network Prevent for Email Server once and only once for each message.

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

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

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

# Proxy server compatibility with Network Prevent for Web

Network Prevent for Web Servers use a standard Internet Content Adaptation Protocol (ICAP) interface and support many proxy servers. Table 3-1 indicates the servers and the protocols.

Symantec Data Loss Prevention also supports secure ICAP (SICAP), using stunnel. See "Secure ICAP support for Network Prevent for Web using the stunnel service" on page 41.

**Table 3-1** Network Prevent for Web supported proxy servers

| Proxy | Supported protocols | Configuration information |
|---|---|---|
| Blue Coat ProxySG version 4.2.1, 5.2.4.8, 5.5.2.1, 5.5.3.1, 6.2.12.1, and 6.5.x for Network Prevent for Web<br>Blue Coat ProxySG version 5.5.3.1 for Mobile Prevent | HTTP, HTTPS, FTP over HTTP, or FTP proxy | Blue Coat product documentation |

**Table 3-1** Network Prevent for Web supported proxy servers *(continued)*

| Proxy | Supported protocols | Configuration information |
|---|---|---|
| Cisco IronPort S-Series version 6.0, 7.1.2 | HTTP, HTTPS, FTP over HTTP | Cisco IronPort product documentation |
| Microsoft TMG 2010 (without service pack, or with SP1 or SP2) on Microsoft Windows 2008 R2 SP1 Enterprise or Standard Edition | HTTP, HTTPS, limited FTP over HTTP/S | See the *Symantec Data Loss Prevention Integration Guide for Microsoft Threat Management Gateway* |
| Secure Computing Secure Web (Webwasher) versions 6.9.x, 7.2, and 7.4 | HTTP, HTTPS, FTP over HTTP, or FTP proxy | Secure Web documentation (particularly the chapter that describes setting up Secure Web with a DLP Solution) |
| Squid Web Proxy version 3.3.x (Linux only) | HTTP | See the *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy* |
| Symantec Web Gateway versions 5.0 and 5.0.2.8 | HTTP, HTTPS | See the *Symantec Web Gateway 5.0 Implementation Guide* |
| Websense Appliance V5000 and V10000, with Websense Web Security version 7.6.0 | HTTP, HTTPS | Does not support redaction.<br>Only supports "Block HTTP/HTTPS".<br>`RESPMOD` is not supported.<br>Websense blocks the traffic only when the size of the Symantec Data Loss Prevention rejection message (in the response rule) is larger than 512 bytes. If the rejection message is less than 512 bytes, an incident is generated but the network traffic is not blocked. |

# Secure ICAP support for Network Prevent for Web using the stunnel service

Symantec has certified Network Prevent for Web to enable secure ICAP (SICAP) communications with the Blue Coat ProxySG server, beginning with Blue Coat ProxySG version 6.2.12.1. The open-source stunnel service acts as an external SSL encryption wrapper to handle encrypted data sent by the Blue Coat ProxySG

server. This secure communications depends on the stunnel service and the OpenSSL toolkit.

For instructions on how to configure secure ICAP functionality with Network Prevent for Web on both Linux and Windows servers, see Symantec Data Loss Prevention Knowledgebase article http://www.symantec.com/docs/TECH220170.

# High-speed packet capture cards

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

**Table 3-2** Supported high-speed packet capture cards

| Card | Version | Driver version |
|---|---|---|
| Endace | DAG_7.5 G2/G4 (PCI-E)<br>**Note:** Endace cards for use with Data Loss Prevention are supported on Linux 64-bit systems only. Endace cards are not supported on Single Server installations. | 4.2.4 |
| Napatech (64-bit hardware only) | NT4E<br>**Note:** Napatech cards are not supported on Single Server installations. | 4.22a (RHEL 5.10 only), 4.22c (Windows Server 2008 R2 only), 4.26a and 4.26c (RHEL 5.x and 6.x, Microsoft Windows Server 2008 R2 and 2012) |

# Data Insight compatibility with Symantec Data Loss Prevention version 12.5

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

**Table 3-3** Supported versions of Symantec Data Insight for Symantec Data Loss Prevention

| Symantec Data Insight Version | DLP version 11.0 | DLP version 11.1 | DLP version 11.5 | DLP version 11.6 | DLP version 12.0 | DLP version 12.5 |
|---|---|---|---|---|---|---|
| 2.0 | Yes | Yes | Yes | Yes | Yes | Yes |
| 2.5 | No | Yes | Yes | Yes. No SharePoint activities included in incident data. | Yes | Yes |
| 3.0 | No | Yes | Yes | Yes | Yes | Yes |
| 3.0 RP1 | No | Yes | Yes | Yes | Yes | Yes |
| 3.0 RP2 | No | Yes | Yes | Yes | Yes | Yes |
| 3.0.1 | No | Yes | Yes | Yes | Yes | Yes |
| 3.0.1 RP1 | No | No | No | Yes (11.6.1) | Yes | Yes |
| 3.0.1 RU1 RP4 | No | No | No | No | Yes | Yes |
| 4.0 | No | No | No | No | Yes | Yes |
| 4.0 RP2 | No | No | No | No | Yes | Yes |
| 4.5 | No | No | No | No | Yes | Yes |

# Symantec Veritas Cluster Server compatibility

Symantec Veritas Cluster Server (VCS) is a high-availability solution that provides failover capabilities for the Symantec Data Loss Prevention Enforce Server and Oracle database hosts. Symantec Data Loss Prevention version 12.5 supports VCS version 5.1 SP2 and 6.0 on Microsoft Windows operating systems, and VCS version 5.1 SP1 and 6.0 Linux 64-bit operating systems.

# Symantec / Symantec Data Loss Prevention integrations

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

**Table 3-4** Symantec product compatibility with Symantec Data Loss Prevention

| Symantec product | Version | Note | DLP version 11.0 | DLP version 11.1 | DLP version 11.5 | DLP version 11.6 | DLP version 12.0 | DLP version 12.5 |
|---|---|---|---|---|---|---|---|---|
| Symantec PGP Universal Gateway Email | 2.63 | | Yes | Yes | Yes | Yes | Yes | No |
| | 3.3.1 | | No | No | No | Yes | Yes | Yes |
| Symantec Messaging Gateway (SMG) | 7.5 | | Yes | Yes | Yes | Yes | No | Yes |
| | 8.0 | | Yes | Yes | Yes | Yes | No | Yes |
| | 10.0.x | | No | No | Yes | Yes | Yes | Yes |
| | 10.5.x | | No | No | No | No | No | Yes |
| Symantec Web Gateway (SWG) | 5.0 | | No | No | Yes | Yes | Yes | Yes |
| | 5.0, 5.0.2.8 | | No | No | Yes | Yes | Yes | Yes |
| Symantec Enterprise Vault | 10.0 | | Yes | Yes | Yes | No | No | No |
| | 10.0.1 | | No | No | Yes | Yes | No | No |
| | 10.0.2 | | No | No | No | No | Yes | No |
| | 10.0.3 | | No | No | No | No | Yes | No |
| | 10.0.4 | | No | No | No | No | No | Yes |
| | 11 | | No | No | No | No | No | Yes |
| Symantec Data Insight | | See "Data Insight compatibility with Symantec Data Loss Prevention version 12.5" on page 42. | | | | | | |
| Symantec Mobile Management (SMM) | 7.1 SPI | | No | No | Yes | Yes | Yes | Yes |

**Table 3-4** Symantec product compatibility with Symantec Data Loss Prevention *(continued)*

| Symantec product | Version | Note | DLP version 11.0 | DLP version 11.1 | DLP version 11.5 | DLP version 11.6 | DLP version 12.0 | DLP version 12.5 |
|---|---|---|---|---|---|---|---|---|
| | 7.2 | | No | No | Yes | Yes | Yes | Yes |
| Symantec Veritas Cluster Server | For Windows 64-bit: 5.1 SP2 | High-availability solution for the Enforce Server and Oracle database.<br>See "Symantec Veritas Cluster Server compatibility" on page 43. | No | Yes | Yes | Yes | Yes | Yes |
| | For Windows 64-bit: 6.0 | | No | No | Yes | Yes | Yes | Yes |
| | For Linux 64-bit: 5.1 SP1 | | No | No | Yes | Yes | Yes | Yes |
| | For Linux 64-bit: 6.0 | | No | No | Yes | Yes | Yes | Yes |
| Symantec Endpoint Protection | 12.1 | For information about configuring Symantec Endpoint Protection for use with Network Discover and Network Monitor, see the Symantec Data Loss Prevention 12.0 Release Notes. | No | No | No | No | Yes | Yes |

# Network Discover compatibility

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

See “Supported file system targets” on page 46.

See “Supported IBM Notes targets” on page 47.

See “Supported SQL database targets” on page 47.

See “Supported SharePoint server targets” on page 47.

See “Supported Exchange Server Web Store connector targets” on page 48.

See “Supported Exchange Server Web Services connector targets” on page 48.

See “Supported file system scanner targets” on page 49.

See “Supported Documentum (scanner) targets” on page 49.

See “Supported Livelink scanner targets” on page 49.

See “Supported Web server (scanner) targets” on page 50.

# Supported file system targets

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

Supported file servers:

- CIFS Servers only

Supported file shares:

- CIFS on Windows Server 2008 and 2012
- NFS on Red Hat Enterprise Linux 5.x and 6.x
- DFS scanning on Windows 2008 and 2012.

**Note:** DFS is not supported with Network Protect.

In addition, the File System target supports scanning of the following file types:

- Microsoft Outlook Personal Folders (`.pst` files) created with Outlook 2007, 2010, and 2013.
  The Network Discover Server scanning this target must be running a Windows operating system, and Outlook 2007 or later must be installed on that system.
- File systems on UNIX systems, even if they are not exposed as CIFS or NFS shares.
  Use the SFTP protocol to provide a method similar to the scans of file shares. You can also scan the local file system on a Linux Network Discover Server by listing the path name in the content root. For example, you can enter `/home/myfiles`.

## Supported IBM Notes targets

The IBM Notes (formerly known as Lotus Notes) target supports scanning of the following versions:

- Lotus Notes 7.0
- Lotus Notes 8.0
- Lotus Notes 8.5.x
- IBM Notes 9.0.x

The files `Notes.jar` and `NCSO.jar` are in the Lotus Notes client installation directory. The manifest version number of these files depend on the Domino server version.

- Version 7 has a manifest version in the JAR file of 1.4.2
- Version 8 has a manifest version in the JAR file of 1.5.0
- Version 9 has a manifest version in the JAR file of 1.6.0

## Supported SQL database targets

The following SQL Databases were tested with Network Discover Target scans:

- Oracle 10g, 11g (11.2.0.4), and 12c (12.1.0.2) (the *vendor_name* is `oracle`)
- SQL Server 2005, 2008 R2, 2012, and 2014 (the *vendor_name* is `sqlserver`)
- DB2 9 (the *vendor_name* is `db2`)

Contact Symantec Data Loss Prevention support for information about scanning any other SQL databases.

## Supported SharePoint server targets

The following SharePoint server targets are supported:

- Microsoft Office SharePoint Server 2007, on Windows Server 2003, 32-bit or 64-bit, or Windows Server 2008 R1, 32-bit or 64-bit
- Microsoft Office SharePoint Server 2010, on Windows Server 2008 R2, 64-bit
- Microsoft Office SharePoint Server 2013, on Windows Server 2008 R2, 64-bit
- Microsoft Office SharePoint Server 2013 SP1, on Windows Server 2012 R2, 64-bit
- Microsoft Office SharePoint Online 2010
- Microsoft Office SharePoint Online 2013

# Supported Exchange Server Web Store connector targets

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

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

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

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

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

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

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

# Supported Exchange Server Web Services connector targets

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

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

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

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

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

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

## Supported file system scanner targets

The following remote Windows systems can be scanned:

- Windows Server 2008
- Windows Server 2012

The following Linux file systems can be scanned:

- Red Hat Enterprise Linux 5.x
- Red Hat Enterprise Linux 6.x

The following AIX file systems can be scanned:

- AIX 5.3
- AIX 6.1

AIX requires the following C run time libraries, as well as Java 1.5 and Java 7 JRE:

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

The following 32-bit Solaris file systems can be scanned (64-bit systems are not supported):

- Solaris 9 (SPARC platform)
- Solaris 10 (SPARC platform)

Solaris requires the following patch levels for the scanner:

- Solaris 9, 115697-01
  http://sunsolve.sun.com/search/document.do?assetkey=1-21-115697-02-1

File systems on UNIX systems can also be scanned using the SFTP protocol. This protocol provides a method similar to share-based file scanning, instead of using the File System Scanner. Contact Symantec Professional Services for details.

## Supported Documentum (scanner) targets

The Documentum scanner supports scanning a Documentum Content Server 5.3.x or 6.6.x repository.

## Supported Livelink scanner targets

The Livelink scanner supports scanning of Livelink Server 9.x targets.

## 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 50.

See "Endpoint Prevent supported applications" on page 52.

## Endpoint Data Loss Prevention supported operating systems

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

**Table 3-5** Endpoint Data Loss Prevention supported operating systems

| Operating system | Version | DLP Version 11.0 | DLP Versions 11.1.x, 11.5, and 11.6 | DLP Version 12.0 | DLP Version 12.5 |
|---|---|---|---|---|---|
| Windows XP Professional (32-bit) | SP2 | Yes | Yes | Yes | No |
| | SP3 | Yes | Yes | Yes | No |
| | SP2 | Yes | Yes | Yes | Yes |
| | R2 | Yes | Yes | Yes | Yes |
| Windows Vista Enterprise (32-bit) | unpatched | No | No | No | No |
| | SP1 | Yes | Yes | Yes | No |
| | SP2 | No | Yes | Yes | No |
| Windows 7 Enterprise, Professional, Ultimate (32-bit) | SP1 | Yes (Windows 7 only, not SP1) | Yes (11.1.1 and later only) | Yes | Yes |

**Table 3-5** Endpoint Data Loss Prevention supported operating systems *(continued)*

| Operating system | Version | DLP Version 11.0 | DLP Versions 11.1.x, 11.5, and 11.6 | DLP Version 12.0 | DLP Version 12.5 |
|---|---|---|---|---|---|
| Windows 7 Enterprise, Professional, Ultimate (64-bit) | SP1 | Yes (Windows 7 only, not SP1) | Yes (11.1.1 and later only) | Yes | Yes |
| Windows 8 Enterprise PC operating system (32-bit) | N/A | No | Yes (11.6.3 and later only) | Yes (12.0.1 and later only) | No |
| Windows 8 Enterprise PC operating system (64-bit) | N/A | No | Yes (11.6.3 and later only) | Yes (12.0.1 and later only) | Yes |
| Windows 8.1 Enterprise PC operating system (64-bit only) | Unpatched | No | No | Yes (12.0.1 and later only) | Yes |
| | Update 1 | No | No | No | Yes |
| | Update 2 | No | No | No | Yes |
| Windows Server 2003 (32-bit) | SP2 | Yes | Yes | Yes | Yes |
| | R2 | No | Yes | Yes | Yes |
| Windows Server 2008 Enterprise or Standard (64-bit) | R2 | No | Yes | Yes | Yes |
| Windows Server 2012 Datacenter, Standard, Essentials, or Foundation (64-bit) | R2 | No | No | No | Yes (Desktop mode only) |
| Apple Mac OS X 10.8 (64-bit) | | No | No | No | Yes |

**Table 3-5** Endpoint Data Loss Prevention supported operating systems *(continued)*

| Operating system | Version | DLP Version 11.0 | DLP Versions 11.1.x, 11.5, and 11.6 | DLP Version 12.0 | DLP Version 12.5 |
|---|---|---|---|---|---|
| Apple Mac OS X 10.9 (64-bit) | | No | No | No | Yes |
| Apple Mac OS X 10.10 (64-bit) | | No | No | No | Yes |

# Endpoint Prevent supported applications

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

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

**Table 3-6** Applications supported by Endpoint Prevent

| Feature | Software | Version | Symantec Data Loss Prevention | | | | |
|---|---|---|---|---|---|---|---|
| | | | Version 10.0 | Version 10.5 | Versions 11.x | Version 12.0 | Version 12.5 |
| HTTP | All browsers | All | Yes | Yes | Yes | Yes | Yes |
| Secure HTTP (HTTPS) | Internet Explorer | 6.0 | Yes | Yes | Yes | Yes | Yes |
| | | 7.0 | Yes | Yes | Yes | Yes | Yes |
| | | 8.0 | Yes | Yes | Yes | Yes | Yes |

**Table 3-6** Applications supported by Endpoint Prevent *(continued)*

| Feature | Software | Version | Symantec Data Loss Prevention | | | | |
|---|---|---|---|---|---|---|---|
| | | | Version 10.0 | Version 10.5 | Versions 11.x | Version 12.0 | Version 12.5 |
| | | 9.0 | No | No | Yes (11.1.1 and later) | Yes | Yes |
| | | 10.0 | No | No | No | Yes (12.0.1 and later) | Yes |
| | | 11.0 | No | No | No | Yes (12.0.1 and later on Windows 8.1 Enterprise only) | Yes (Windows 7 and 8.1 Enterprise, EPM disabled) |
| | Firefox | 2.0 | Yes | Yes | Yes | Yes | No |
| | | 3.0 | Yes | Yes | Yes | Yes | No |
| | | 3.5 | Yes | Yes | Yes | Yes | No |
| | | 3.6 | No | Yes | Yes | Yes | No |
| | | 4.0 | No | No | Yes (11.1.1 and later) | Yes | No |
| | | 5.0 | No | No | Yes (11.6 and later, through Application Monitoring [AFAC]) | Yes (through Application Monitoring [AFAC]) | No |
| | | 23 through 32 | No | No | No | No | Yes |
| Instant messaging | Yahoo Messenger | 7.5 | Yes | Yes | Yes | Yes | Yes |
| | | 8.0 | Yes | Yes | Yes | Yes | Yes |
| | | 8.1 | Yes | Yes | Yes | Yes | Yes |
| | | 9.0 | Yes | Yes | Yes | Yes | Yes |
| | | 10.0 | No | Yes | Yes | No | Yes |
| | | 11.0 | No | No | No | No | Yes |

**Table 3-6** Applications supported by Endpoint Prevent *(continued)*

| Feature | Software | Version | Symantec Data Loss Prevention | | | | |
|---|---|---|---|---|---|---|---|
| | | | Version 10.0 | Version 10.5 | Versions 11.x | Version 12.0 | Version 12.5 |
| | MSN Messenger | 8.1 | Yes | Yes | Yes | Yes | No |
| | | 9.0 (14) | Yes | Yes | Yes | Yes | No |
| | AIM | 5.9 | Yes | Yes | Yes | Yes | Yes |
| | | 6.0 | Yes | Yes | Yes | Yes | Yes |
| | | 6.1 | Yes | Yes | Yes | Yes | Yes |
| | | 6.5 | Yes | Yes | Yes | Yes | Yes |
| | | 6.8 | Yes | Yes | Yes | Yes | Yes |
| | | 6.9 | Yes | Yes | Yes | Yes | Yes |
| | AIM Pro | 1.4 | Yes | Yes | Yes | Yes | Yes |
| | | 1.5 | Yes | Yes | Yes | Yes | Yes |
| Email | Outlook | 2002 | Yes | Yes | Yes | Yes | No |
| | | 2003 | Yes | Yes | Yes | Yes | Yes |
| | | 2007 | Yes | Yes | Yes | Yes | Yes |
| | | 2010 | No | No | Yes | Yes | Yes |
| | | 2013 | No | No | No | No | Yes |
| | Outlook Web Access (rich and light mode) | 2007 | No | No | No | No | Yes |
| | | 2010 | No | No | No | No | Yes |
| | | 2013 | No | No | No | No | Yes |
| | Outlook.com | | No | No | No | No | Yes |
| | Eudora | | No | No | No | No | No |

**Table 3-6** Applications supported by Endpoint Prevent *(continued)*

| Feature | Software | Version | Symantec Data Loss Prevention | | | | |
|---|---|---|---|---|---|---|---|
| | | | Version 10.0 | Version 10.5 | Versions 11.x | Version 12.0 | Version 12.5 |
| | Thunderbird | | No | No | No | No | No |
| | Lotus Notes | 6.5 | No | Yes | Yes | Yes | Yes |
| | | 7.0 | Yes | Yes | Yes | Yes | Yes |
| | | 8.0 | Yes | Yes | Yes | Yes | Yes |
| | | 8.5 | Yes | Yes | Yes | Yes | Yes |
| | | 8.5.1 | No | No | Yes (11.1.1 and later) | Yes | Yes |
| | | 8.5.3 | No | No | Yes (11.1.1 and later) | Yes | Yes |
| FTP | | | Yes | Yes | Yes | Yes | Yes |
| CD/DVD | BsClip | | Yes | Yes | Yes | Yes | Yes |
| | Bs Recorder Gold | | Yes | Yes | Yes | Yes | Yes |
| | BurnAware | | Yes | Yes | Yes | Yes | Yes |
| | Cheetah Burner | | Yes | Yes | Yes | Yes | Yes |
| | Command Burner | | Yes | Yes | Yes | Yes | Yes |
| | CopyToDVD | | Yes | Yes | Yes | Yes | Yes |
| | Creator10 | | Yes | Yes | Yes | Yes | Yes |
| | Deep Burner (32-bit Windows XP) | | Yes | Yes | Yes | Yes | No |

**Table 3-6** Applications supported by Endpoint Prevent *(continued)*

| Feature | Software | Version | Symantec Data Loss Prevention | | | | |
|---|---|---|---|---|---|---|---|
| | | | Version 10.0 | Version 10.5 | Versions 11.x | Version 12.0 | Version 12.5 |
| | GEAR for Windows | | Yes | Yes | Yes | Yes | Yes |
| | mkisofs | | Yes | Yes | Yes | Yes | Yes |
| | Nero | | Yes | Yes | Yes | Yes | Yes |
| | NeroStartSmart | | Yes | Yes | Yes | Yes | Yes |
| | Roxio | | Yes | Yes | Yes | Yes | Yes |
| | Roxio RecordNow | | Yes | Yes | Yes | Yes | Yes |
| | Roxio5 | | Yes | Yes | Yes | Yes | Yes |
| | Roxio Mediahub | | Yes | Yes | Yes | Yes | Yes |
| | Silent Night Micro Burner | | Yes | Yes | Yes | Yes | Yes |
| | Star Burn | | Yes | Yes | Yes | Yes | Yes |
| | Windows native CD/DVD writer | | No | No | Yes | Yes | Yes |

# Mobile Prevent compatibility

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

Mobile Prevent is not supported on Single Server installations.

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

Mobile Prevent supports the following Web applications through the Safari Web browser for iPads and iPhones (for iOS versions 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3, and 7). This table also lists the supported type of response rules available for each Web application. See the *Symantec Data Loss Prevention Administration Guide* for more information on creating policies and response rules.

**Table 3-7** Web applications supported by Mobile Prevent

| Application | iOS version | Symantec Data Loss Prevention version | Available Mobile Prevent Response Rules | | |
|---|---|---|---|---|---|
| | | | Notification | Block | Content Removal |
| AOL | 4.3.x | 12.0 | Yes | Yes | Yes |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | Yes | Yes |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | Yes | Yes |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | No | No | No |
| | 7 | 12.5 | Yes | No | No |
| Facebook | 4.3.x | 12.0 | Yes | Yes | Yes |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | Yes | Yes |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | Yes | Yes |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | No | No | No |
| | 7 | 12.5 | No | No | No |
| Gmail | 4.3.x | 12.0 | Yes | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | No | No |

**Table 3-7** Web applications supported by Mobile Prevent *(continued)*

| Application | iOS version | Symantec Data Loss Prevention version | Available Mobile Prevent Response Rules | | |
|---|---|---|---|---|---|
| | | | Notification | Block | Content Removal |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | Yes | No | No |
| | 7 | 12.5 | Yes | No | No |
| Windows Live Mail | 4.3.x | 12.0 | Yes | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | No | No |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | No | No | No |
| | 7 | 12.5 | No | No | No |
| Yahoo! Mail | 4.3.x | 12.0 | Yes | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | No | No |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | Yes | Yes | Yes |
| | 7 | 12.5 | Yes | Yes | Yes |
| Twitter | 4.3.x | 12.0 | Yes | Yes | Yes |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.0 | Yes | Yes | Yes |

**Table 3-7** Web applications supported by Mobile Prevent *(continued)*

| Application | iOS version | Symantec Data Loss Prevention version | Available Mobile Prevent Response Rules | | |
|---|---|---|---|---|---|
| | | | Notification | Block | Content Removal |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.0 | Yes | Yes | Yes |
| | 7 | 12.0 | No | No | No |
| | 4.3.x | 12.5 | No | No | No |
| | 5.0, 5.0.1, 5.1, 5.1.1 | 12.5 | No | No | No |
| | 6.0, 6.0.1, 6.1, 6.1.2, 6.1.3 | 12.5 | No | No | No |
| | 7 | 12.5 | No | No | No |

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

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

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

- Netflix for iPad application

# Mobile Email Monitor compatibility

The following two tables provide compatibility information for Mobile Email Monitor.

Table 3-8 list the Microsoft Exchange ActiveSync versions that are compatible with Symantec Data Loss Prevention Mobile Email Monitor on various devices.

**Note:** Symantec Data Loss Prevention Mobile Email Monitor is not supported on Single Server installations.

**Table 3-8** Microsoft Exchange ActiveSync versions compatible with Mobile Email Monitor

| ActiveSync Versions | Devices | Mail Applications |
|---|---|---|
| Microsoft Exchange ActiveSync 2003 | Samsung Galaxy S3<br>HTC<br>Google<br>Motorola | Android native email |
| Microsoft Exchange ActiveSync 2007 | iPad<br>iPhone<br>Samsung Galaxy S3<br>HTC<br>Google<br>Motorola | iOS native email<br>Android native email |
| Microsoft Exchange ActiveSync 2010 | iPad<br>iPhone<br>Samsung Galaxy S3<br>HTC<br>Google<br>Motorola | iOS native email<br>Android native email |

Table 3-9 lists the devices and operating systems that are compatible with Symantec Data Loss Prevention Mobile Email Monitor.

**Table 3-9** Mobile devices and operating systems and compatible with Mobile Email Monitor

| Device | Operating systems |
|---|---|
| iPhone | iOS |
| iPad | iOS |
| Samsung Galaxy S3 | Android Jelly Bean 4.1, 4.2, 4.3 |
| HTC | Android Jelly Bean 4.1, 4.2, 4.3 |
| Google | Android Jelly Bean 4.1, 4.2, 4.3 |

**Table 3-9** Mobile devices and operating systems and compatible with Mobile Email Monitor *(continued)*

| Device | Operating systems |
|---|---|
| Motorola | Android Jelly Bean 4.1, 4.2, 4.3 |