Symantec
A Division of Broadcom

Symantec Data Loss Prevention System Requirements and Compatibility Guide

Version 15.7

Last updated: September 22, 2020

Table of Contents

About this guide

About updates to Symantec Data Loss Prevention system requirements

System requirements are occasionally updated as new information becomes available. Refer to Table 1: Change history for the system requirements for a summary of the latest changes.

The following table provides the history of updates to system requirements.

Table 1: Change history for the system requirements

Date	Description
22 September 2020	Added support for Oracle 19c Database Release Update 19.8.0.0. Added support for Citrix XenApp 7.15 LTSR CU6 and Citrix XenDesktop 7.15 LTSR CU6.
14 September 2020	Added support for VMware Horizon View 7.12 Added support for Oracle 19c Database Release Update 19.6.0.0 (only on Linux servers). Corrected support for Chrome 85 on Windows for DLP Agent version 15.5 MP1.
3 September 2020	Added support for Edge (Chromium-based) through version 85. Added support for Chrome 85 on both Windows and macOS.
31 August 2020	Added support for Firefox 80 on both Windows and macOS.
27 August 2020	Clarified support for Oracle 19c (for Enterprise Edition and Standard Edition) to include 19.3.0.0.0.
25 August 2020	Corrected support for Chrome 75 on Windows endpoints to include support on Symantec Data Loss Prevention version 15.5 MP1.
20 August 2020	Corrected support for Citrix XenDesktop 7 2003 to indicate support with Windows 10 20H1 (version 2004).
17 August 2020	Added support for Citrix XenApp 7 2003 and Citrix XenDesktop 7 2003.
3 August 2020	Added support for Firefox 79 on both Windows and macOS.
31 July 2020	Added support for Oracle 19c (for Oracle 19c Enterprise Release 1 and Oracle 19c Standard Edition).
23 July 2020	Support for macOS 10.15.6 on DLP Agents.
16 July 2020	Added support for Chrome 84 on both Windows and macOS.
10 July 2020	Corrected details about number of patches that are required for running Windows Server 2012 R2. Added topic macOS 11 compatibility and testing.
1 July 2020	Added support for the Microsoft Exchange Server 2019 server target. Added support for Firefox 77 and 78 on both Windows and macOS.
10 June 2020	Removed references to the Symantec Support Portal and pointed relevant links to the Tech Docs Portal.
4 June 2020	Added support for Red Hat Enterprise Linux 7.8 for operating systems for servers.
2 June 2020	Added support for macOS 10.15.5 on DLP Agents.
29 May 2020	Added support for Chrome 83 on both Windows and macOS. Removed references to Chrome 83 beta support. Added support for Windows 10 Version 2004 (OS build 19041.264) on DLP Agents.
15 May 2020	Added support for Firefox 76 on both Windows and macOS. Removed references to Firefox 76 beta support. Added support for Data Insight 6.1.5. Added support for the following Napatech Driver packages: • Windows: 11.8.1 • Linux: 12.1

Date	Description
23 April 2020	Added content from TECH235226 (see Support for Monitoring Applications Protected by System Integrity Protection) Added known issues that are associated with Firefox 75 and macOS 10.15.4. Added support information for the following browsers in beta: • Firefox 76 (for macOS) • Firefox 76.0.0.7415 (for Windows) • Chrome 83.0.4103.14 (for Windows and macOS)
9 April 2020	Added support for Chrome 81 on both Windows and macOS. Added support for Firefox 75 on both Windows and macOS. Added support for macOS 10.15.4 on DLP Agents. Added support for the following EMDI, EDM, and IDM Remote Indexer platforms: • Red Hat Enterprise Linux 6.8, 6.9, and 6.10 • Red Hat Enterprise Linux 7.3 through 7.7 • Oracle Linux 7.3 and 7.6 Added information on default SIP support and included steps to update SIP settings.
24 March 2020	Removed support for SICAP for the McAfee Web Gateway proxy.
17 March 2020	Added support for Firefox 74 on macOS.
21 February 2020	Added support for Firefox 73 on both Windows and macOS.
19 February 2020	Added support for VMware Horizon View 7.11 for DLP Agents.
14 February 2020	Added support for macOS 10.15.3 on DLP Agent version 15.7.

About deprecated platforms

Certain platforms are referred to as “deprecated.” That indicates that while the deprecated platform is supported in the current release, Symantec plans to remove support in an upcoming release. If your Symantec Data Loss Prevention environment includes a deprecated platform, you should plan on updating the platform to a later supported version or a different supported platform as soon as possible.

System requirements and recommendations

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)
- The system requirements for your Symantec Data Loss Prevention installation

The effect of scale on system requirements

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 Enforce Server users
- Number of detection servers
- Daily incident volume
- Amount of network traffic to monitor
- Size of Exact Data Match profile (EDM), Exact Match Data Identifier profile (EMDI), or Indexed Data Match profile (IDM)
- Size of your Form Recognition profile

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

Table 2: Types of enterprise deployments

Variable	Single tier	Very small (minimum supported system)	Small	Medium	Large
Number of Enforce Server users	N/A	5	10	20	30
Number of detection servers	N/A	5	10	50	100+
Daily incident volume	N/A	5000	10,000	50,000	100,000
Volume of network traffic to monitor	30-40 Mbps	30-40 Mbps	30-40 Mbps	30-40 Mbps	>40 Mbps
EDM/EMDI/IDM index size	EDM 4 million cells or IDM 250 MB (1400 files). See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing for enterprise deployments.	See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing for enterprise deployments.	See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing for enterprise deployments.	See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing for enterprise deployments.	See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing for enterprise deployments.
Form Recognition profile size	See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.	See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.	See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.	See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.	See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.
Hardware requirements	Single-tier installation minimum hardware requirements	Very small installation minimum hardware requirements	Small installation minimum hardware requirements	Medium installation minimum hardware requirements	Large enterprise minimum hardware requirements

For additional related information see also *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines*, available at the Tech Docs Portal.

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.

- Single-tier installation minimum hardware requirements
- Very small installation minimum hardware requirements
- Small installation minimum hardware requirements
- Medium installation minimum hardware requirements
- Large enterprise minimum hardware requirements
- Operating system requirements for servers

> **NOTE**
>
> Requirements for Symantec Data Loss Prevention Virtual Appliances are the same as for the software server counterparts, except for virtual environment support. Virtual server support

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

Oracle database requirements

Single-tier installation minimum hardware requirements

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

Because single-tier deployments include the Enforce Server, the Oracle database, and the detection server all on the same computer, the processing and memory requirements are higher than they might be on dedicated servers in a two- or three-tier deployment.

> **NOTE**
>
> The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see article Guidelines for tuning Symantec Data Loss Prevention to scan large files at the Tech Docs Portal for information about tuning your system for large file inspection.

Table 3: Single-tier installation minimum hardware requirements

Required for	Single Server Installation
Processor	Eight-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)

Very small installation minimum hardware requirements

The following table provides the system requirements for the smallest supported installation of Symantec Data Loss Prevention. This is a two-tier installation, in which the Enforce Server and Oracle database are both hosted on the same computer.

NOTE

The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see Guidelines for tuning Symantec Data Loss Prevention to scan large files at the Tech Docs Portal for information about tuning your system for large file inspection.

Table 4: Very small installation minimum hardware requirements

Required for	Enforce Server	Network Monitor	Network Discover, Network Prevent, Cloud Prevent for Email, or Endpoint Prevent
Processor	Two-core CPU	Four-core CPU	Four-core CPU
Memory	8 GB RAM	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)
Disk	500 GB hard drive storage. 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 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	One 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.

Small installation minimum hardware requirements

The following table provides the system requirements for a small installation of Symantec Data Loss Prevention. This is a three-tier installation, in which the Enforce Server and Oracle database are hosted on separate computers.

NOTE

The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see article Guidelines for tuning Symantec Data Loss Prevention to scan large files at the Tech Docs Portal for information about tuning your system for large file inspection.

Table 5: Small installation minimum hardware requirements

Required for	Enforce Server	Oracle database	Network Monitor	Network Discover, Network Prevent, Cloud Prevent for Email, or Endpoint Prevent
Processor	Two-core CPU	Two-core CPU	Four-core CPU	Four-core CPU
Memory	8 GB RAM	8 GB RAM	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)
Disk	500 GB hard drive storage. 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.	500 GB - 1 TB Oracle database requirements	140 GB	140 GB 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	One copper or fiber 1 Gb/100 Mb Ethernet NIC to communicate with detection servers.	N/A	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.

Medium installation minimum hardware requirements

The following table provides the system requirements for medium installations of Symantec Data Loss Prevention. This is a three-tier installation, with the Enforce Server and Oracle database hosted on separate computers.

> **NOTE**
>
> The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see Guidelines for tuning Symantec Data Loss Prevention to scan large files at the Tech Docs Portal for information about tuning your system for large file inspection.

Table 6: Medium installation minimum hardware requirements

Required for	Enforce Server	Oracle database	Network Monitor	Network Discover, Network Prevent, Cloud Prevent for Email, or Endpoint Prevent
Processor	Two-core CPU	Four-core CPU	Four-core CPU	Four-core CPU
Memory	12 GB RAM (EDM/IDM and Form Recognition profile size can increase memory requirements. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)	16 GB RAM	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)	6–8 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance at the Tech Docs Portal for information about Form Recognition sizing.)
Disk	500 GB hybrid storage. 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.	500 GB - 1 TB Oracle database requirements	140 GB	140 GB 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.	N/A	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.

Oracle database requirements

The effect of scale on system requirements

Large enterprise minimum hardware requirements

The following table provides the system requirements for large installations of Symantec Data Loss Prevention. This is a three-tier installation, with the Enforce Server and Oracle database hosted on separate computers.

NOTE

The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see Guidelines for tuning Symantec Data Loss Prevention to scan large files about tuning your system for large file inspection.

Table 7: Large enterprise minimum system requirements

Required For	Enforce Server	Oracle database	Network Monitor	Network Discover, Network Prevent, Cloud Prevent for Email, or Endpoint Prevent
Processor	Four-core CPU	Six-core CPU	Eight-core CPU	Eight-core CPU
Memory	16 GB RAM (EDM/IDM and Form Recognition profile size can increase memory requirements. See the *Symantec Data Loss Prevention Administration Guide* for information about EDM and IDM sizing. See Form Recognition sizing and performance for information about Form Recognition sizing.	32 GB RAM	8–16 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance for information about Form Recognition sizing.	8–16 GB RAM (See the *Symantec Data Loss Prevention Administration Guide* for information about EDM, IDM, and EMDI impact on sizing. See Form Recognition sizing and performance for information about Form Recognition sizing.
Disk Requirements	1 TB storage (SSD or SAN) 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.	500 GB - 1 TB Oracle database requirements	140 GB	140 GB 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: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC	N/A	To communicate with the Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet For network traffic monitoring (pick one): 1 copper or fiber 1 Gb/100 Mb Ethernet NIC.	To communicate with the Enforce Server: 1 copper or fiber 1 Gb/100 Mb Ethernet NIC
High-speed packet capture cards	N/A	N/A	High-speed packet capture cards	N/A

Oracle database requirements

The effect of scale on system requirements

Operating system requirements for servers

Symantec Data Loss Prevention servers can be installed on a supported Linux or Windows operating system. Different operating systems can be used for different servers in a heterogeneous environment.

Symantec Data Loss Prevention supports the following 64-bit operating systems for Enforce Server and detection server computers:

- Microsoft Windows Server 2012 R2, Datacenter Edition with patches
  Installing patches for Windows Server 2012 R2
- Microsoft Windows Server 2012 R2, Standard Edition with patches
  Installing patches for Windows Server 2012 R2
- Microsoft Windows Server 2016, Standard Edition
- Microsoft Windows Server 2016, Datacenter Edition
- Red Hat Enterprise Linux 6.8, 6.9, and 6.10
  Installing fonts on Linux servers
- Red Hat Enterprise Linux 7.3 through 7.8
  Installing fonts on Linux servers
- Oracle Linux 7.3 and 7.6
  Installing fonts on Linux servers

Symantec Data Loss Prevention supports the 64-bit operating system for detection server computers on Microsoft Windows Server 2016, Core.

Operating system requirements for Single Server deployments

Symantec Data Loss Prevention supports the following 64-bit operating systems for Single Server deployments:

- Microsoft Windows Server 2012 R2, Datacenter Edition with patches
  Installing patches for Windows Server 2012 R2
- Microsoft Windows Server 2012 R2, Standard Edition with patches
  Installing patches for Windows Server 2012 R2
- Microsoft Windows Server 2016, Standard Edition
- Microsoft Windows Server 2016, Datacenter Edition
- Red Hat Enterprise Linux 6.8, 6.9, and 6.10
  Installing fonts on Linux servers
- Red Hat Enterprise Linux 7.3 through 7.8
  Installing fonts on Linux servers
- Oracle Linux 7.3 and 7.6
  Installing fonts on Linux servers

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

Supported languages for detection

See also the *Symantec Data Loss Prevention Administration Guide* for detailed information about supported languages and character sets. You can find the *Symantec Data Loss Prevention Administration Guide* at the Tech Docs Portal.

Operating system requirements for the domain controller agent

The domain controller agent enables you to resolve user names from IPv4 addresses in HTTP/S and FTP incidents. See the *Symantec Data Loss Prevention Installation Guide* for domain controller agent installation details.

Symantec Data Loss Prevention supports the following operating systems for the domain controller agent:

- Microsoft Windows Server 2012, Datacenter Edition (64-bit)
- Microsoft Windows Server 2012, Standard Edition (64-bit)
- Microsoft Windows Server 2012 R2, Datacenter Edition with patches
  Installing patches for Windows Server 2012 R2
- Microsoft Windows Server 2012 R2, Standard Edition with patches
  Installing patches for Windows Server 2012 R2

Installing patches for Windows Server 2012 R2

If you use Windows Server 2012 R2, you must install three Microsoft patches: KB2919355, KB2919442, and KB2999226.

Go to https://support.microsoft.com/en-us/kb/2919355 and install KB2919355.

Go to https://support.microsoft.com/en-us/kb/2919442 and install KB2919442.

Go to https://support.microsoft.com/en-us/kb/2999226 and install KB2999226.

Installing fonts on Linux servers

You must have at least one font installed on your Linux servers. However, Symantec recommends installing all available fonts on your Linux servers if you intend to use Form Recognition detection. To install all available fonts, run: `yum groupinstall fonts` on each Linux Enforce and detection server.

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.

Linux partition minimum size guidelines—Enforce Server without a database, or detection server

Table 8: 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 installations	Contains installed programs such as Symantec Data Loss Prevention, the Oracle server, and the Oracle database. The Oracle database requires significant space in this directory. For improved performance, you may want to mount this partition on different disks/SAN/RAID from where the root partition is mounted.
`/var`	15 GB for Small/Medium installations 46 GB for Large installations	Contains logs, EDM/IDM indexes, Form Recognition indexes, incremental scan indexes, and network packet capture directories. **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).

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

Table 9: Linux partition minimum size guidelines—Enforce Server without a database, or detection server

Partition	Minimum size guidelines	Description and comments
`/opt`	10 GB	Contains installed programs such as Symantec Data Loss Prevention and the Oracle client.
`/var`	15 GB for Small/Medium installations 46 GB for Large installations	Contains logs, EDM/IDM indexes, Form Recognition indexes, incremental scan indexes, and network packet capture directories. **Note:** The `/var/spool/pcap` and `/var/Symantec/DataLossPrevention/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.

Installing fonts on Linux servers

You must have at least one font installed on your Linux servers. However, Symantec recommends installing all available fonts on your Linux servers if you intend to use Form Recognition detection. To install all available fonts, run: `yum groupinstall fonts` on each Linux Enforce and detection server.

System requirements for OCR Servers

Operating system requirements for OCR Servers

Symantec supports deployment of OCR Servers on the Windows operating system. The same Windows servers supported for installation of the Enforce Server are supported for installation of OCR Servers.

Operating system requirements for servers

For more information on OCR Server system requirements and sizing guidelines, see Using the OCR Server Sizing Estimator Spreadsheet.

Symantec Data Loss Prevention compatibility with OCR Servers

OCR Server version 1 is compatible with the following Symantec Data Loss Prevention versions:

- 15.0
- 15.1
- 15.5
- 15.7

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.

- Windows operating system requirements for endpoint systems
- macOS operating system requirements for endpoint systems
- Memory and disk space requirements for the Symantec DLP Agent

Windows operating system requirements for endpoint systems

Support assumes that you have installed the latest DLP hot fix from Symantec (where applicable).

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

- Table 10: Windows Server
- Table 11: Windows 7
- Table 12: Windows 8
- Table 13: Windows 10 Enterprise, Pro PC operating system (64-bit) operating systems

Table 10: Windows Server

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Windows Server 2003 SP2 R2	Yes	No	Yes	No	No	No	No
Windows Server Enterprise or Standard (64-bit) 2008 R2	Yes	Yes	Yes	Yes	Yes	Yes	No
Windows Server Enterprise or Standard (64-bit) 2012 R2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Windows Server 2016 Standard or Datacenter Edition (64-bit) No service pack	No	No	Yes (on DLP Agent versions 14.6 MP1 and MP2)	Yes	Yes	Yes	Yes
Microsoft Windows Server 2019 (64-bit) No	No	No	No	No	No	Yes	Yes

Table 11: Windows 7

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Windows 7 Enterprise, Professional, Ultimate (32-bit) No service pack	Yes	Yes	Yes	No	No	No	No
Windows 7 Enterprise, Professional, Ultimate (32-bit) SP1	Yes	Yes	Yes	Yes	Yes	Yes	No
Windows 7 Enterprise, Professional, Ultimate (64-bit) No service pack	Yes	Yes	Yes	No	No	No	No
Windows 7 Enterprise, Professional, Ultimate (64-bit) SP1	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 12: Windows 8

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Windows 8 Enterprise PC operating system (32-bit)	No	No	No	No	No	No	No
Windows 8 Enterprise PC operating system (64-bit)	Yes	Yes	Yes	No	No	No	No
Windows 8.1 Enterprise, Pro PC operating system (64-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 8.1 Enterprise, Pro PC operating system (64-bit) Update 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Windows 8.1 Enterprise, Pro PC operating system (64-bit) Update 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 8.1 Enterprise, Pro PC operating system (64-bit) Update 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 13: Windows 10 Enterprise, Pro PC operating system (64-bit) operating systems

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Unpatched	Yes (14.0.1)	Yes	Yes	Yes	No	No	No
Version 1511 (November Update)	No	Yes	Yes	Yes	Deprecated	Deprecated	No
Version 1607 (Anniversary Update)	No	Yes	Yes	Yes	Deprecated	Deprecated	
Version 1703 (Creators Update)[a]	No	No	Yes (on DLP Agent version 14.6 MP1 and MP2)	Yes	Yes	Yes	Yes
Version 1709 (Fall Creators Update)	No	No	Yes (on DLP Agent version 14.6 MP1 and MP2)	Yes	Yes	Yes	Yes
Version 1803 (April 2018 Update) [build #17134.48]	No	No	No	Yes (on DLP Agent version 15.0 MP1)	Yes	Yes	Yes
Version 1607 LTSB	No	No	No	No	Yes (on DLP Agent version 15.1 MP1)	Yes	Yes
Version 1809 (Creators Update)	No	No	No	No	Yes (on DLP Agent version 15.1 MP1)	Yes	Yes
Version 1903 (May 2019 Update)	No	No	Yes (on DLP Agent version 14.6 MP3)	No	Yes (on DLP Agent version 15.1 MP2)	Yes (on DLP Agent version 15.5 MP1)	Yes

[a] See Known Issues for DLP Agent Support of Microsoft Windows 10 Creators Update

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Version 1909 (November 2019 Update)[b]	No	No	No	No	Yes (on DLP Agent version 15.1 MP2)	Yes (on DLP Agent version 15.5 MP2)	Yes
Version 2004 (OS build 19041.264)[c]					Yes	Yes	Yes

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

About Endpoint Data Loss Prevention compatibility

About Symantec Management Platform server requirements

macOS operating system requirements for endpoint systems

Support assumes that you have installed the latest DLP hot fix from Symantec (where applicable).

See Endpoint known issues for a list of the latest known issues.

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

Table 14: Endpoint Data Loss Prevention supported macOS operating systems

Operating system	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Apple macOS 10.8 (64-bit)	Yes	No	No	No	No	No	No
Apple macOS 10.9 (64-bit)	Yes	Yes	Yes	No	No	No	No
Apple macOS 10.10 (64-bit)	Yes	Yes	Yes	Deprecated	No	No	No
Apple macOS 10.11 (64-bit)	No	Yes	• Through 10.11.5 • 10.11.6 on 14.6 MP2	• Through 10.11.5 • 10.11.6 on on 15.0 MP1	Yes	Yes	No
Apple macOS 10.12 (64-bit)	No	Yes (on DLP Agent version 14.5 MP1)	• Through 10.12.5 on DLP Agent version 14.6 MP1 • 10.12.6 on 14.6 MP2	• Through 10.12.5 • 10.12.6 on 15.0 MP1	Yes	Yes	Yes

[b] There are known issues with monitoring drag and drop activity for Edge on Windows 10 (Version 1909). You must apply a hot fix for support of the Edge browser.

[c] Edge monitoring on Windows 10 Version 2004 (OS build 19041.264) is supported on DLP Agent version 15.7 MP1. Edge monitoring is not supported with DLP Agent versions 15.1, 15.5, and 15.7.

Operating system	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Apple macOS 10.13 (64-bit)[a, b]	No	No	• 10.13.1 on DLP Agent version 14.6 MP2 • 10.13.2 on 14.6 MP2 [c] • 10.13.3 on 14.6 MP2 with 10.13.4 on 14.6 MP2 with	• 10.13.1 on DLP Agent version 15.0 • 10.13.2 on version 15.0 • 10.13.3 on version 15.0 • 10.13.4 on version 15.0 MP1 • 10.13.5 on version 15.0 MP1 • 10.13.6 on version 15.0 MP1	Yes (through 10.13.6)	Yes (through 10.13.6)	Yes (through 10.13.6)
Apple macOS 10.14 (64-bit)[d]	No	No	10.14.5 on version 14.6 MP3	No	10.14.1, 10.14.2, and 10.14.5 on version 15.1 MP2	10.14.1 - 10.14.4 on version 15.5 10.14.5 on version 15.5 MP1 10.14.6 on 15.5 MP1	10.14.1 - 10.14.5
Apple macOS 10.15 (64-bit)[e]					10.15.1 - 10.15.6 on version 15.1 MP2	10.15.1 - 10.15.6 on version 15.5 MP2	10.15.1 - 10.15.4 10.15.5 and 1015.6 on 15.7 MP1

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

macOS 11 compatibility and testing

Apple has announced that, in the upcoming release of macOS 11, kernel extensions will be replaced by system extensions. System extensions are a more secure alternative to kernel extensions because third-party code runs in the user space instead of in the kernel. This change in architecture protects the operating system by eliminating third-party access to the kernel, while simultaneously granting a high level of privilege to third-party applications through system extensions.

In response to the introduction of system extensions in macOS, Symantec is migrating the DLP Agent to the system extensions architecture. To ensure the same level of functionality and data protection as previously, Symantec is testing the new DLP Agent with macOS 11 beta builds.

To continue monitoring endpoints that have upgraded to macOS 11, you will need to deploy the new DLP Agent, which will be based on the version 15.7 agent. Compatibility with macOS 11 will be introduced in Symantec Data Loss Prevention 15.7 Maintenance Pack 2, available in the fall or early winter of 2020. Previous versions of the DLP Agent will not be supported with macOS 11.

Update August 6, 2020:

[a] See Known issues using macOS 10.13 with DLP Agent versions 14.6 MP2 through 15.5

[b] See Known issues upgrading from macOS 10.13.6 to macOS 10.14 with DLP Agent version 15.1

[c] See DLP Agents deployed with MDM profiles on macOS 10.13.2 and later not loading

[d] See Known issues upgrading from macOS 10.13.6 to macOS 10.14 with DLP Agent version 15.1

[e] See Configuring MDM profiles for Full Disk Access for macOS 10.15 and DLP Agent support

Symantec has completed testing macOS 11 Developer Beta 3 with the rearchitected DLP Agent (in development). Aside from the system extensions changes that are already known, Symantec has not encountered other changes that could adversely impact the DLP Agent.

Going forward, Symantec will continue testing with new beta releases when they are released, and will continue to rebuild the macOS agent to support system extensions with the upcoming release.

Additional updates will be published here if there are significant testing results of beta versions of macOS 11 interoperability with the rearchitected DLP Agent to share with Data Loss Prevention Endpoint customers.

Update August 26, 2020:

Symantec has completed testing macOS 11 Developer Beta 5 with the rearchitected DLP Agent (in development).

Developer Beta 5 does not include certain third-party libraries that are required for the DLP Agent service to start. Symantec is investigating alternatives to resolve this issue.

Update September 11, 2020:

Symantec has resolved the issue caused by the removal of certain third-party libraries in Developer Beta 5 and Public Beta 2 and has begun testing with Public Beta 3.

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.

> **NOTE**
>
> The default content size for detection is 30 MB. If you plan to scan files larger than 30 MB, see Guidelines for tuning Symantec Data Loss Prevention to scan large files at the Tech Docs Portal for information about tuning your system for large file inspection.

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 that are found in content in these languages:

- Arabic
- Brazilian Portuguese
- Chinese (traditional)
- Chinese (simplified)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Spanish
- Swedish
- Turkish*

*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.
- 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 that 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. Contact Symantec Technical Support for additional information on language-related enhancements or plans for the languages not listed.

About support for character sets, languages, and locales

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_15.7_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_15.7_Lang_Pack_<language>.zip
```

Language packs and corresponding locale codes lists available language packs.

Table 15: Language packs and corresponding locale codes

Language	Locale code
Brazilian Portuguese	`PT_BR`
Chinese (Simplified)	`ZH_CN`
Chinese (Traditional)	`ZH_TW`
French	`FR_FR`
German	`DE_DE`
Italian	`IT_IT`
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

Symantec Data Loss Prevention supports the following Oracle databases:

- Oracle 19c Enterprise (19.3.0.0.0).
  Support is included for the following Database Release Updates (RUs):
  - 19.6.0.0 (only on Linux servers)
  - 19.8.0.0

  You must obtain software and support from Oracle. For implementation details, see the *Symantec Data Loss Prevention Oracle 19c Implementation Guide* at the Tech Docs Portal.
- Oracle 19c Standard Edition (19.3.0.0.0). Support is included for the following Database Release Updates (RUs):
  Support is included for the following Database Release Updates (RUs):
  - 19.6.0.0 (only on Linux servers)
  - 19.8.0.0

  You can obtain the software from Symantec. For implementation details, see the *Symantec Data Loss Prevention Oracle 19c Implementation Guide* at the Tech Docs Portal.
- Oracle 12c Enterprise Edition
  Oracle 12.1.0.2 and 12.2.0.1 are tested with the Symantec Data Loss Prevention schema. You must obtain software and support from Oracle. For implementation details, see the *Symantec Data Loss Prevention Oracle 12c Enterprise Implementation Guide* at the Tech Docs Portal.
- Oracle 12c Standard Edition 2 (12c SE2) (12.1.0.2)
- Oracle 12c Standard Edition 2 Release 2 (12c SE2 R2) (12.2.0.1)
  Symantec provides Oracle 12.2.0.1 Standard Edition with Symantec Data Loss Prevention.
  See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* to install Oracle at the Tech Docs Portal.

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.

See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* to install Oracle with the provided template and scripts.

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 single-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 12c Client on the Enforce Server computer to communicate with the remote Oracle 12c SE2 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.
  Single-tier installation minimum hardware requirements
  Very small installation minimum hardware requirements

If you install Oracle 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 2012 R2 Standard, Enterprise, or Datacenter (64-bit)
  - Microsoft Windows Server 2016 Standard or Datacenter (64-bit)
  - Red Hat Enterprise Linux 6.9 (64-bit)
  - Red Hat Enterprise Linux 7.3 through 7.5 (64-bit)
  - Oracle Linux 7.3 or Oracle Linux 7.3 with RHCK (Red Hat compatible kernel)
- 8-32 GB of RAM
- 8-16 GB of swap space (equal to RAM up to 16 GB)
- 500 GB – 1 TB of disk space for the Enforce database

On a Linux system, if the Oracle database is on the same computer as the Enforce Server, then the `/opt` file system must have at least 500 GB of free space for small or medium installations. 1 TB of free space is required for 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 Server 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 10 or 11
- Mozilla Firefox 62 through 69, and Firefox Enterprise (ESR) 68.
- Google Chrome 75 through 79

You must be using Adobe Flash Player, minimally version 27, to view the Folder Risk Report for Network Discover (**Incidents > Discover > Folder Risk Report**).

Deploying Data Loss Prevention on public cloud infrastructures

Symantec supports deployment of Data Loss Prevention servers on the following public clouds:

- Amazon Web Services (AWS)
  Deploying Symantec Data Loss Prevention on Amazon Web Services infrastructure
- Microsoft Azure
  Deploying Symantec Data Loss Prevention on Microsoft Azure
- Oracle Cloud public clouds
  Deploying Symantec Data Loss Prevention on Oracle Cloud

Deploying Symantec Data Loss Prevention on Amazon Web Services infrastructure

Table 16: Deploying Symantec Data Loss Prevention 12.5 - 15.7 on AWS lists the servers and operating systems that are supported for deployment of Data Loss Prevention on AWS. You can run Symantec Data Loss Prevention on AWS on supported operating systems.

Minimum system requirements for Symantec Data Loss Prevention servers

Table 16: Deploying Symantec Data Loss Prevention 12.5 - 15.7 on AWS

Data Loss Prevention servers
Enforce Server with Oracle database on the same computer (two-tier deployments) Oracle database with Amazon RDS (three-tier deployments) Cloud Prevent for Email Network Prevent for Web Network Prevent for Email Endpoint Prevent Network Discover API Detection for Developer Apps Appliance

For more information, see *Deploying the Symantec Data Loss Prevention on Amazon Web Services (AWS) Infrastructure* at the Tech Docs Portal.

Deploying Symantec Data Loss Prevention on Microsoft Azure

Deploying Symantec Data Loss Prevention on Microsoft Azure lists the servers that are supported for deployment of Data Loss Prevention on Microsoft Azure. You can run Symantec Data Loss Prevention on Microsoft Azure on supported operating systems.

Minimum system requirements for Symantec Data Loss Prevention servers

Table 17: Deploying Symantec Data Loss Prevention on Microsoft Azure

Data Loss Prevention servers
Enforce Server with Oracle database Cloud Prevent for Email Network Prevent for Web Network Prevent for Email Endpoint Prevent Network Discover

Symantec supports SIR (Symantec Image Recognition) including OCR and Form Recognition with Cloud Prevent for Email on Azure.

Symantec supports the use of the Azure load balancer to balance the endpoint client connections to the Endpoint Server.

Deploying Symantec Data Loss Prevention on Oracle Cloud

Symantec Data Loss Prevention is supported in the following environments:

- Oracle Cloud IaaS
- Oracle Bare Metal Cloud with managed Virtual Machine (VM) instances

Deploying Symantec Data Loss Prevention on Oracle Cloud Infrastructure as a Service lists the servers that are supported for deployment of Data Loss Prevention on Oracle Cloud Infrastructure as a Service. You can run Symantec Data Loss Prevention on Oracle Cloud on supported operating systems.

Minimum system requirements for Symantec Data Loss Prevention

Table 18: Deploying Symantec Data Loss Prevention on Oracle Cloud Infrastructure as a Service

Data Loss Prevention servers
Enforce Server with Oracle database on the same computer (two-tier deployments) Network Prevent for Email Endpoint Prevent Network Discover

NOTE

Three-tier Symantec Data Loss Prevention deployments are not supported on Oracle.

Virtual machine support

The following lists virtual machine support:

- Virtual server support
  Virtual server support
- Virtual desktop and virtual application support with Endpoint Prevent
  Virtual desktop and virtual application support with

Virtual server support

Symantec supports running Symantec Data Loss Prevention servers on VMware ESXi 6.x and Windows Hyper-V virtualization products, provided that the virtualization environment is running a supported operating system.

NOTE

Symantec Data Loss Prevention Virtual Appliances are supported in a virtualization environment on VMware ESXi 5.5.0 Update 2 and VMware ESXi 6.5.

Operating system requirements for servers

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

System requirements for Symantec Data Loss Prevention servers

Consider the following support information when configuring a virtual server environment:

- 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 VMware ESXi 5.x, VMware ESXi 5.x, and VMware ESX 6.x virtual hardware. If you deploy the Enforce Server to a virtual machine, you must install the Oracle database using physical server hardware.
- Symantec supports running the Enforce Server and Oracle database server in a Windows Hyper-V environment.
- Symantec does not support Single Server installations on virtual machines.

A variety of factors influence virtual machine performance, 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 Tech Docs Portal 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 to monitor virtual desktops and prevent remote users from copying sensitive data that is accessible through a virtual desktop.

Citrix virtualization support

The DLP agent is supported to run on the following Citrix XenDesktop virtual workstations and Citrix XenApp server configurations:

- Citrix XenApp
  - Citrix XenApp 7.6 on Windows Server 2008 Enterprise Edition R2 (64-bit) and Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.9 on Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.11 on Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.12 Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.13 Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.14 Windows Server 2012 R2 Standard Edition
  - Citrix XenApp 7.15 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7.15 Long Term Service Release (LTSR), Update 2 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7.15 LTSR, Cumulative Update (CU) 6 on Windows Server 2016 Standard Edition with Symantec Data Loss Prevention 15.7 MP1
  - Citrix XenApp 7.16 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7.17 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7.18 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7.19 on Windows Server 2016 Standard Edition
  - Citrix XenApp 7 2003 on Windows Server 2019 Standard Edition

    NOTE

    Files saved from Microsoft Office (using Save As) to client drives hosted on Citrix XenApp 7.13 through 7.18 and Citrix XenApp 7 2003 are not monitored. However, if you are running Citrix XenApp 7.13 or later with version 7.12 Virtual Delivery Agent (VDA), files saved to client drives (using Save As) are monitored. You can find steps on enabling monitoring for these save operations. See Known issue running Citrix XenApp and XenDesktop versions 7.13 through 7.18 at the Tech Docs Portal.
- Citrix XenDesktop
  - Citrix XenDesktop 7.9 on Windows 8.0, 8.1, and Windows 10 (64-bit)
  - Citrix XenDesktop 7.12 on Windows 10 (64-bit)
  - Citrix XenDesktop 7.12 on Windows 10 (64-bit)
  - Citrix XenDesktop 7.14 on Windows 10 (64-bit)
  - Citrix XenDesktop 7.15 on Windows 10 RS2 (64-bit)
  - Citrix XenDesktop 7.15 Long Term Service Release (LTSR), Update 2 on Windows 10 RS4 (version 1803) (64-bit)
  - Citrix XenDesktop 7.15 LTSR, CU 6 on Windows 10 (version 2004) with Symantec Data Loss Prevention 15.7 MP1
  - Citrix XenDesktop 7.16 on Windows 10 RS2 (64-bit)
  - Citrix XenDesktop 7.17 on Windows 10 RS3 (version 1703) (64-bit)
  - Citrix XenDesktop 7.18 on Windows 10 RS4 (version 1803) (64-bit)
  - Citrix XenDesktop 7.19 on Windows 10 RS4 (version 1803) (64-bit)
  - Citrix XenDesktop 7 2003 on Windows 10 20H1 (version 2004) (64-bit)

    NOTE

    Files saved from Microsoft Office (using Save As) to client drives hosted on Citrix XenDesktop 7.13 through 7.18 and Citrix XenDesktop 7 2003 are not monitored. However, if you are running Citrix XenDesktop 7.13

or later with version 7.12 Virtual Delivery Agent (VDA), files saved to client drives (using **Save As**) are monitored. See Known issue running Citrix XenApp and XenDesktop versions 7.13 through 7.18 at the Tech Docs Portal.

VMware virtualization support

Symantec supports running the Symantec DLP Agent software on virtual workstations using one of the following:

- VMware Workstation 6.5.x

  NOTE

  VMware Workstation 6.5.x is deprecated in Symantec Data Loss Prevention 15.0.
- VMware View 4.6
- VMware Horizon View:
  - 6.0.1
  - 6.2.1
  - 7.1
  - 7.3.1
  - 7.4
  - 7.6
  - 7.9–7.12
- VMware Fusion 7 (macOS)
- Hyper-V and Hyper-V (WS 2012 R2)

Supported operating systems for the EMDI, EDM, and IDM Remote Indexers

You can install the Remote EMDI Indexer, the Remote EDM Indexer, and the Remote IDM Indexer on all Windows and Linux platforms that are supported for installing the Enforce Server and detection servers. In addition, you can install the indexers on the following Windows endpoint operating systems:

- Windows 8.1 (64-bit) Enterprise, Professional
- Windows 8.1 Update 1 (64-bit) Enterprise, Professional
- Windows 8.1 Update 2 (64-bit) Enterprise, Professional
- Windows 8.1 Update 3 (64-bit) Enterprise, Professional
- Windows 10 Update [1511] (64-bit] Enterprise, Professional
- Windows 10 Red Stone Update [1607 - RS1] (64-bit] Enterprise, Professional
- Microsoft Windows 10 Creators Update (RS2 v1703)
- Microsoft Windows 10 Creators Update (RS3 v1709)
- Microsoft Windows 10 Creators Update (RS4 v1803)

Third-party software requirements and recommendations

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

- Required third-party software for required software
- Required Linux RPMs for required Linux RPMs
- Recommended third-party software for recommended software

Table 19: Required third-party software

Software	Required for	Description
Adobe Reader	All systems	Adobe Reader is required for reading the Symantec Data Loss Prevention documentation. Download from http://www.adobe.com.
Apache Tomcat version 9	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) JRE 1.8.0_202	All servers	You install the JRE from Symantec Data Loss Prevention software ZIP files.
Flex SDK 4.6	Network Discover Server	Required SDK for Folder Risk Reporting.
Napatech driver package 8.0.3 (driver version 3.5.1) (Windows Server 2012 R2 and Windows Server 2016) and driver package 8.1.0 (driver version 3.5.0) (RHEL 6x/7x)	Napatech NT20E2, NT4E, NT40A01, and NT40E3 high-speed packet capture card	Provides high-speed monitoring. Symantec supports • Multiple capture ports per Napatech Network capture card • NT40A01 Napatech Network Accelerator • NT40E3 and NT20E2 10 gigabit interfaces • Multi-threaded packet capture • Napatech hardware filtering • Napatech third-generation card drivers for Windows and RHEL platforms • Virtualized Data Loss Prevention Network Monitor with capture cards as PCI pass-through devices in the VMware ESXi platform Napatech cards are not supported on Single Server installations.
WinPcap 4.1.3	Required for Windows-based Network Monitor Server. WinPcap 4.1.3 is required for Microsoft Windows Server 2012. Recommended for all Windows-based detection servers.	Windows packet capture library. Download from http://www.winpcap.org/install/default.htm.
NPcap 0.99xx	Can be used in place of WinPcap for Windows-based Network Monitor Server.	During the Symantec Data Loss Prevention installation, select WinPcap compatibility mode.
Endace card driver 5.3.1	Detection servers equipped with an Endace network measurement card.	Endace cards are not supported on Single Server installations. Download from http://www.endace.com. Medium installation minimum hardware requirements
VMware	Required to run supported components in a virtualized environment. Virtual server support	Virtualization software. Download from https://www.vmware.com/download/vi.
Microsoft Active Directory 2012, 2012 R2, or 2016	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 Required Linux RPMs.

Table 20: Required Linux RPMs

Linux-based servers	Required RPMs

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

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

Red Hat Enterprise Linux version 6 has these additional dependencies:

- Desktop Platform Development group package (`yum groupinstall "Desktop Platform Development"`)
- compat-openldap
- compat-expat1
- compat-db43
- openssl098e

Red Hat Enterprise Linux version 7 has these additional 64-bit only package dependencies:

- Server with GUI group package (`yum groupinstall "Server with GUI"`)
- Dev Tools group package (`yum groupinstall "Development Tools"`)
- compat-openldap
- compat-db
- libpng
- compat-libtiff3
- gtk+-devel
- gtk2-devel
- gstreamer
- libstdc++.so.5
- libX11
- libXext
- libXi
- libXrender
- libXtst
- wget
- unzip

NOTE

SeLinux must be disabled on all Linux-based servers.

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

Table 21: Recommended third-party software

Software	Location	Description
Wireshark	Any server computer	Use Wireshark (formerly Ethereal) to verify that the detection server NIC receives the correct traffic from the SPAN port or tap. You can also use Wireshark to diagnose network problems between other servers. Download the latest version from http://www.wireshark.org.
dagsnap	Network Monitor Server computers that use Endace cards	Use in combination with Wireshark to verify that the detection server Endace NIC receives the correct traffic from the SPAN port or tap. Dagsnap is included with Endace cards, and is not required with non-Endace cards.
Sysinternals Suite	Any Windows server computer	Troubleshooting utilities. Recommended for diagnosing problems on Windows server computers. Download the latest version from http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx.
LDAP browser	Enforce Server	An LDAP browser is recommended for configuring or troubleshooting Active Directory or LDAP.

Product compatibility

Environment compatibility and requirements for Network Prevent for Email

The Cloud 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.

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

Cloud 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 Cloud 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 Cloud Prevent for Email* for information about configuring TLS support for Cloud 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 22: Network Prevent for Web supported proxy servers indicates the servers and the protocols.

Symantec Data Loss Prevention also supports secure ICAP (SICAP). You can set up secureICAP with Blue Coat ProxySG through the Enforce Server administration console. You can set up other proxies with secure ICAP using stunnel. See Secure ICAP support for Network Prevent for Web

Table 22: Network Prevent for Web supported proxy servers

Proxy	Supported protocols	Configuration information
Blue Coat ProxySG versions 6.6.x and6.7 for Network Prevent for Web	ICAP, SICAP, HTTP, HTTPS, or FTP proxy	Blue Coat product documentation
Cisco IronPort S-Series versions 9.1.x, 10.1.x, and 10.5.x	ICAP, HTTP, HTTPS	Cisco IronPort product documentation 9.1.x and 10.5.x support Secure ICAP 10.1.x does not support SICAP
F5 BIG-IP System version 12.0.x, 13.1.0.8, 14.1.0	ICAP, HTTP, HTTPS	See Using the F5 Proxy with Symantec Data Loss Prevention Network Prevent for Web for information on integrating the F5 BIG-IP System with Network Prevent for Web as an ICAP client-server solution.
Fortinet FortiGate-VM 5.6.x and 6.2.x	ICAP, HTTP, HTTPS	FortiGate-VM product documentation
McAfee Web Gateway (formerly Secure Computing Secure Web Webwasher) version 7.7.x, 7.8.x	ICAP, HTTP, HTTPS, or FTP proxy	Secure Web documentation (particularly the chapter that describes setting up Secure Web with a DLP Solution)
Squid Web Proxy versions 3.5.x	ICAP, HTTP, HTTPS	See the *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy*
Websense Appliance V5000 and V10000, with Websense Web Security version 8.4	ICAP, HTTP, HTTPS, FTP	Does not support redaction. Only supports "Block HTTP/HTTPS". `RESPMOD` is not supported. Websense blocks the traffic only when the size of the Symantec Data Loss Prevention rejection message (in the response rule) is larger than 512 bytes. If the rejection message is less than 512 bytes, an incident is generated but the network traffic is not blocked.

SSL monitoring with Network Monitor

Symantec has certified Network Monitor to monitor Blue Coat SSL Visibility Appliance.

For details, see Using the Blue Coat SSL Visibility Appliance with Network Monitor at the Tech Docs Portal.

Secure ICAP support for Network Prevent for Web

You configure your system to use integrated Secure ICAP for Network Prevent for Web. See the *Symantec Data Loss Prevention Administration Guide* for configuration details.

High-speed packet capture cards

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

Table 23: Supported high-speed packet capture cards

Card	Version	Driver version
Endace	DAG 7.5 G2/G4 (PCI-E) DAG 10X2 **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.	5.7.1
Napatech	NT20E2, NT20E3, NT4E, NT40A01, and NT40E3	Symantec Data Loss Prevention supports the following drier pacakges: • Driver package 8.0.3 (driver version 3.5.1) and 11.8.1 (driver version 3.15.x) for Windows • Driver package 8.1.0 (driver version 3.5.0) and 12.1 (driver version 3.19.x) for Linux Symantec Data Loss Prevention supports the following: • Multiple capture ports per Napatech Network capture card • NT40A01 Napatech Network Accelerator • Multi-threaded packet capture • Napatech hardware filtering • Napatech third-generation card drivers for Windows and RHEL platforms • 10 gigabit adapters • Virtualized Data Loss Prevention Network Monitor with capture cards as PCI pass-through devices in the VMware ESXi platform

Veritas Data Insight compatibility with Symantec Data Loss Prevention

Veritas 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. Data Insight provides a connection from the Enforce Server to a Data Insight Management Server.

Table 24: Supported versions of Veritas Data Insight and Symantec Data Loss Prevention

Data Insight version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
2.0 - 4.5.1	No	No	No	No	No	No	No
4.5.2, 4.5.3	Yes	No	No	No	No	No	No
5.0	Yes	Yes	No	No	No	No	No
5.1	Yes	Yes	No	No	No	No	No
5.1.1	No	No	Yes	Yes	Yes	Yes	Yes
5.2	No	No	Yes	Yes	Yes	Yes	Yes
6.0	No	No	Yes, on version 14.6 MP1	Yes	Yes	Yes	Yes

Data Insight version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
6.1	No	No	Yes, on version 14.6 MP2	Yes	Yes	Yes	Yes
6.1.1	No	No	No	Yes, on version 15.0 MP1	Yes	Yes	Yes
6.1.2	No	No	No	No	Yes	Yes	Yes
6.1.3	No	No	No	No	Yes, on version 15.1 MP1	Yes	Yes
6.1.4	No	No	No	No	No	Yes	Yes
6.1.5	No	No	No	No	No	No	Yes

Integrations with other Symantec products

This section describes compatibility of various integrations of Symantec Data Loss Prevention with the following Symantec products:

- Symantec PGP Universal Gateway Email
  Table 25: Symantec PGP Universal Gateway Email
- Symantec Messaging Gateway (SMG)
  Table 26: Symantec Messaging Gateway (SMG) (8200 and 8300 Series)
- Symantec Web Gateway (SWG)
  Table 27: Symantec Web Gateway (SWG)
- Symantec Endpoint Protection
  Table 28: Symantec Endpoint Protection
- Symantec Encryption Management Server (DLP Encryption Insight)
  Table 29: Symantec Encryption Management Server (DLP Encryption Insight)

Table 25: Symantec PGP Universal Gateway Email

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
2.63	No	No	No	No	No	No	No
3.3.x	Yes	Yes	No	Yes	Yes	Yes	Yes

Table 26: Symantec Messaging Gateway (SMG) (8200 and 8300 Series)

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
7.5	No	No	No	No	No	No	No
8.0	No	No	No	No	No	No	No
10.0.1.2	Yes	Yes	No	Yes	No	No	No
10.0.2	Yes	Yes	No	Yes	No	No	No
10.5.0-8	Yes	Yes	No	Yes	No	No	No
10.5.3	Yes	Yes	No	No	No	No	No

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
10.6.x	No	No	Yes	Yes	Yes	Yes	Yes
10.7.x	No	No	No	No	No	Yes	Yes

Table 27: Symantec Web Gateway (SWG)

Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
5.0, 5.0.2.8	Yes	Yes	No	No	No	No	No
5.2.7	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 28: Symantec Endpoint Protection

Version	Note	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
12.1, 12.1 RU4	For information about configuring Symantec Endpoint Protection for use with Network Discover and Network Monitor, see the Symantec Data Loss Prevention 14.0 Release Notes.	Yes	No	No	No	No	No	No
12.1.5 (12.1 RU5)		Yes	Yes	Yes	No	No	No	No
12.1.6 (12.1 RU6 MP6)		No	No	Yes	Yes	Yes	Yes	Yes
14.0		No	No	No	Yes	Yes	Yes	Yes
14.0.1 and 14.0.1 MP1		No	No	No	Yes	Yes	Yes	Yes

Table 29: Symantec Encryption Management Server (DLP Encryption Insight)

Symantec product	Version	DLP version 14.0	DLP version 14.5	DLP version 14.6	DLP version 15.0	DLP version 15.1	DLP version 15.5	DLP version 15.7
Symantec Encryption Management Server (DLP Encryption Insight)	3.3	Yes	Yes	Yes	Yes	No	No	No
	3.4	No	No	Yes	Yes	Yes	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.

The following lists scan support for enterprise data repositories:

- Supported Box cloud storage targets
- Supported file system targets
- Supported IBM (Lotus) Notes targets
- Supported SQL database targets
- Supported SharePoint server targets
- Supported Exchange Server targets
- Supported file system scanner targets
- Supported Exchange scanner targets
- Supported Documentum (scanner) targets
- Supported OpenText (Livelink) scanner targets
- Supported web server (scanner) targets

Supported Box cloud storage targets

The Box target supports scanning of files and folders in enterprise Box cloud storage accounts.

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:
  - Windows Server 2012 R2 (SMB 1.0 and 2.0 supported on Windows and Linux Network Discover servers)
  - Windows Server 2016 (SMB 1.0 and 2.0 supported on Windows and Linux Network Discover servers)
- NFS on Red Hat Enterprise Linux 7.x
- DFS scanning on Windows 2012 R2 and 2016.

  NOTE

  DFS is not supported with Network Protect.

In addition, the File System target supports scanning of Microsoft Outlook Personal Folders (`.pst` files) created with Outlook 2010, 2013, and 2016.

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.

> **NOTE**
>
> You can use SSHFS to scan File System targets on UNIX systems. Ensure that you use Fuse components and packages that are validated and adhere to your organisation's security policies. Technical support is available only for Symantec components.

Supported IBM (Lotus) Notes targets

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

- 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 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 11g (11.2.x), 12c (12.1.x), and 18c (12.2.x) (the vendor_name is `oracle`)
- SQL Server 2014 and 2016 (the vendor_name is `sqlserver`)
- DB2 10.5 (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 2010 SP2
- Microsoft Office SharePoint Server 2013 SP1
- Microsoft Office SharePoint Server 2016
- Microsoft Office SharePoint Server 2019

  Consider the following known issues when implementing the SharePoint Server 2019 server target:
  - Symantec Data Loss Prevention cannot scan a SharePoint Server 2019 target if any folder name or file name on the SharePoint site contains the percentage sign (%) or the number sign (#).
  - Symantec Data Loss Prevention does not support quarantine and encrypt remediations for SharePoint Server 2019.
  - You must install the Symantec SharePoint solution to scan SharePoint Server 2019 targets.

Supported Exchange Server targets

Symantec Data Loss Prevention supports the following Exchange Server targets:

- Microsoft Exchange Server 2010 SP3
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 2016 (on-premises)
- Microsoft Exchange Server 2019

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 2013 and 2016 Personal Archives.

Supported file system scanner targets

The following remote Windows systems can be scanned:

- Windows Server 2012 R2
- Windows Server 2016

The following Linux file systems can be scanned:

- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 7.4

The following AIX file systems can be scanned:

- AIX 7.1

AIX requires the following C run time libraries, as well as Java 1.8 and Java 8 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 10 (SPARC platform)

Solaris requires the following patch levels for the scanner:

- Solaris 9, 115697-01

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, and 6.7 repository.

Supported OpenText (Livelink) scanner targets

The Livelink scanner supports scanning of OpenText (Livelink) Server 9.x targets. This version is deprecated in Symantec Data Loss Prevention 15.5. Livelink scanners will be removed in the next release of Symantec Data Loss Prevention.

Supported web server (scanner) targets

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

Endpoint Prevent supported applications

Applications supported by Endpoint Prevent on Windows describes individual applications that can be monitored using Endpoint Prevent on Windows; Applications supported by Endpoint Prevent on macOS describes browsers that can be monitored using Endpoint Prevent on macOS.

Endpoint Prevent enables you to add monitoring support for other third-party applications not listed in the following tables. An example of a third-party application is Thunderbird. You add monitoring support for an application on the Enforce Server administration console. Always test monitoring support for 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.

> **NOTE**
>
> Applications supported by Endpoint Prevent on Windows and Applications supported by Endpoint Prevent on macOS assume that you have installed the latest DLP hot fix from Symantec.

Applications Supported by Endpoint Prevent on Windows

This section describes individual applications that can be monitored using Endpoint Prevent on Windows.

NOTE

Support assumes that you have installed the latest DLP hot fix from Symantec (where applicable).

Support is listed for the following items:

- Table 30: HTTP support
- Table 31: Secure HTTP (HTTPS)
- Table 32: Instant messaging
- Table 33: Email
- Table 34: FTP
- Table 35: CD/DVD
- Table 36: Cloud Sync Apps
- Table 37: Misc.

Table 30: HTTP support

Software	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
All browsers	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 31: Secure HTTP (HTTPS)

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Internet Explorer 6.0	No	No	No	No	No	No	No
Internet Explorer 7.0	No	No	No	No	No	No	No
Internet Explorer 8.0	No	No	No	No	No	No	No
Internet Explorer 9.0	Yes	Yes	Yes	Yes (Windows Server 2008 R2)	No	No	No
Internet Explorer 10.0	Yes	Yes	Yes	Yes (Windows Server 2008 R2)	Yes	Yes	Yes
Internet Explorer 11.0	Yes (Windows 7, 8.1 Enterprise, 10 Enterprise, and Windows Server 2012 R2, Desktop mode only and EPM disabled)	Yes (Windows 7, 8.1 Enterprise, 10 Enterprise, and Windows Server 2012 R2, Desktop mode only and EPM disabled)	Yes	Yes	Yes	Yes	Yes

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Edge RS1	No	No	Yes No (on Windows 10 Creators Update [versions 1703 and 1709]. The table below provides details on enabling Edge monitoring for this scenario.)	Yes No (on Windows 10 Creators Update [versions 1703 and 1709]. The table below provides details on enabling Edge monitoring for this scenario.)	Deprecated	No	No
Edge RS2	No	No	No	No	Yes	Yes	Yes
Edge RS3 and RS4	No	No	No	No	Yes	Yes	Yes
Edge (Chromium-based) through version 85	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes, on version 15.7 MP1
Firefox 2.0 - 5.0	No	No	No	No	No	No	No
Firefox 23 through 46.0.1	Yes (35 through 46.0.1 and through 47.0 on DLP Agent version 14.0.2)	Yes	Yes (38-44), including Firefox 64-bit, which was introduced in Firefox 43.	Yes	Yes	Yes	Yes
Firefox 51-54	No	No	Yes	Yes	Yes	Yes	Yes
Firefox 56-61	No	No	Yes	Yes	Yes	Yes	Yes
Firefox 62	No	No	No	Yes	Yes	Yes	Yes
Firefox 63	No	No	No	No	Yes, on version 15.1 MP1	Yes	Yes
Firefox 64, 65	No	No	No	No	No	Yes	Yes
Firefox 66	No	No	Yes, on version 14.6 MP3	Yes, on version 15.0 MP1	Yes, on version 15.1 MP1	Yes	Yes
Firefox 67	No	No	Yes, on version 14.6 MP3	No	Yes, on version 15.1 MP1	Yes, on version 15.5 MP1	Yes
Firefox 68	No	No	Yes, on version 14.6 MP3	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Firefox 69	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Firefox 70	No	No	No	No	Yes	Yes	Yes
Firefox 71	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes
Firefox 73-80	No	No	No	No	Yes	Yes	Yes

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Chrome 38 through 59	Yes (51 and 52 supported on Windows 10 with DLP Agent version 14.0.2)	Yes (Windows 10 support begins with 51) 55 on DLP Agent version 14.5 MP1	38-44, 51-57 58 and 59 on DLP Agent version 14.6 MP1	Yes	Yes	Yes	Yes
Chrome 60 through 69	No	No	Yes	Yes	Yes	Yes	Yes
Chrome 70, 71	No	No	No	No	Yes, on version 15.1 MP1	Yes	Yes
Chrome 72, 73	No	No	Yes See ALERT2641 for details.	Yes See ALERT2641 for details.	Yes, on version 15.1 MP1 See ALERT2641 for details.	Yes See ALERT2641 for details.	Yes
Chrome 74	No	No	No	No	No	Yes, with version 15.5 MP1	Yes
Chrome 75	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP	Yes
Chrome 76	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Chrome 77	No	No	No	Yes, on version 15.0 MP1	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Chrome 78-81	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes
Chrome 83-85	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes

Table 32: Instant messaging

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
AIM	N/A	Yes	Yes	Yes	Yes	Yes	Yes
AIM Pro	N/A	Yes	Yes	Yes	Yes	Yes	Yes
AIM6	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Office Comm-unicator	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Skype	N/A	Yes	Yes	Yes	Yes	Yes	Yes

Table 33: Email

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Outlook 2007	Yes	No	No	No	No	No	No
Outlook 2010	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Software and version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Outlook 2013	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Outlook 2016	No	Yes	Yes	Yes	Yes	Yes	Yes
Outlook 2019	No	No	No	No	Yes, on 15.1 MP1	Yes	Yes
Outlook Web Access (rich and light mode) 2007	Yes	No	No	No	No	No	No
Outlook Web Access (rich and light mode) 2010	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Outlook Web Access (rich and light mode) 2013		Yes	Yes	Yes	Yes	Yes	Yes
Outlook Web Access (rich and light mode) 2016	No	Yes	Yes	Yes	Yes	Yes	Yes
Lotus Notes	6.5 - 8.5	No	No	No	No	No	No
Lotus Notes (IBM Domino)	8.5.x	Yes	Yes (8.5.3)	Yes (8.5.3)	Yes (8.5.3)	Yes (8.5.3)	Yes (8.5.3)
Lotus Notes (IBM Domino)	9.x	Yes	Yes	Yes	Yes	Yes	Yes

Table 34: FTP

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 35: CD/DVD

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
BsClip	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Bs Recorder Gold	N/A	Yes	Yes	Yes	Yes	Yes	Yes
BurnAware	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Cheetah Burner	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Command Burner	N/A	Yes	Yes	Yes	Yes	Yes	Yes
CopyToDVD	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Creator10	N/A	Yes	Yes	Yes	Yes	Yes	Yes

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
GEAR for Windows	N/A	Yes	Yes	Yes	Yes	Yes	Yes
mkisofs	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Nero	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Nero Start Smart	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Roxio	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Roxio RecordNow	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Roxio5	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Roxio Mediahub	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Silent Night Micro Burner	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Star Burn	N/A	Yes	Yes	Yes	Yes	Yes	Yes

Table 36: Cloud Sync Apps

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Box 4.0.6169	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Box (Most recent version available)					Yes	Yes	Yes
Dropbox 3.2.x, 6.4.x, 8.4.x 12.4.x, 13.4.x, 14.4.x, 15.4.x, 17.4.x, 19.4.x, 20.4.x - 38.4.x	Yes Version 3.2.9	Yes Version 20.4.x - 29.4.x supported on DLP Agents version 14.5 MP1.	Yes Version 20.4.x - 29.4.x supported on DLP Agents version 14.6 MP1.	Yes Version 20.4.x - 38.4.x.	Yes Version 31.4.x - 38.4.x	Yes	Yes
Dropbox (Most recent version available)					Yes	Yes	Yes
Microsoft OneDrive 15.0.4675. 1003 for Win 8.1 (default) 17.3.4726. 0226 and 17.3.6517. 0809 for Win 7 x86/x64 (desktop client)	Yes	Yes, and OneDrive Personal and OneDrive for Business 17.3.6390. 0509, 17.3.6517. 0809	Yes	Yes	Yes	Yes	Yes
Hightail 2.4.7. 1621	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Google Backup and Sync 3.35.x		Yes	Yes	Yes	Yes	Yes	Yes
Google Backup and Sync 3.37.x				Yes	Yes	Yes	Yes
Google Backup and Sync 3.41.x					Yes	Yes	Yes
Google Backup and Sync 3.46.x							Yes
Google Drive 1.20.x, 1.30.x, 1.32.x, 2.34.x - 3.37.x	Yes, 1.20.x	Yes Version 2.34.x supported on DLP Agents version 14.5 MP1.	Yes Version 2.34.x supported on DLP Agents version 14.6 MP1.	Yes	Yes	Yes	Yes
Apple iCloud 4.0.3.56, 4.0.5.20	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 37: Misc.

Software version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Adobe Reader	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Apple iTunes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Click-to-Run Microsoft Pro 2013	No	Yes	Yes	Yes	Yes	Yes	Yes
Roxio_ Central	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WebEx Communications Module	Yes	Yes	Yes	Yes	Yes	Yes	Yes

NOTE

Version 14.6.x and 15.0 agents running on Windows 10 Creators Update (versions 1703 and 1709) do not support monitoring Edge by default. Known Issues for DLP Agent Support of Microsoft Windows 10 Creators Update at the Tech Docs Portal provides details on enabling Edge monitoring for this scenario.

Applications Supported by Endpoint Prevent on macOS

This section describes individual applications that can be monitored using Endpoint Prevent on macOS.

NOTE

Support assumes that you have installed the latest DLP hot fix from Symantec (where applicable).

See Endpoint known issues for a list of the latest known issues.

Support is listed for the following items:

- Table 38: Secure HTTP (HTTPS)
- Table 39: Email
- Table 40: Instant messaging

Table 38: Secure HTTP (HTTPS)

Software Version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Firefox 36.0.4, ESR 31.XFirefox	Yes	Yes	Yes	No	No	Yes	Yes
Firefox 38 ESR, 45 ESR, 45.1.1 ESR, 45.4.0, 46.0.1 ESR, 49.0.2 ESR	No	No	Yes	Yes	Yes	Yes	Yes
Firefox 68 ESR	No	No	No	No	No	No	Yes
Firefox 49 and 50	No	Yes (on DLP Agents, version 14.5 MP1)	Yes	Yes	Yes	Yes	Yes
Firefox 51-54	No	No	Yes	Yes	Yes	Yes	Yes
Firefox 56-61	No	No	Yes	Yes	Yes	Yes	Yes
Firefox 62	No	No	No	Yes	Yes	Yes	Yes
Firefox 63	No	No	No	No	Yes, on version 15.1 MP1	Yes	Yes
Firefox 64, 65	No	No	No	No	No	Yes	Yes
Firefox 66	No	No	Yes, on version 14.6 MP3	Yes, on version 15.0 MP1	Yes, on version 15.1 MP1	Yes	Yes
Firefox 67	No	No	Yes, on version 14.6 MP3	No	Yes, on version 15.1 MP1	Yes, on version 15.5 MP1	Yes
Firefox 68	No	No	Yes, on version 14.6 MP3	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Firefox 69	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Firefox 70	No	No	No	No	Yes	Yes	Yes
Firefox 71	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes
Firefox 73-80	No	No	No	No	Yes	Yes	Yes
Safari 6.0.x, 7.0.x., and 8.0.x	Yes	No	No	No	No	No	No
Safari 9.1	No	Yes (on macOS 10.11)	Yes	Yes	No	No	No

Software Version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Safari 10.0.x	No	Yes (for DLP Agents, version 14.5 MP1 on macOS 10.11.6)	Yes	Yes	Yes	Yes	No
Safari 10.1.x	No	No	Yes (for DLP Agents, version 14.6 MP1 on macOS 10.11.6) No (on macOS 10.12.4)	Yes (on macOS 10.11.x, 10.12.1, 10.12.2, and 10.12.3) No (on macOS 10.12.4, 10.12.5, and 10.12.6)	Yes (macOS 10.11, 10.12.1, 10.12.2, and 10.12.3)	Yes	Yes
Safari 11			No	No	Yes (on macOS 10.12.4 and later)	Yes	Yes
Safari 12				No	Yes (on macOS 10.12.6 and later starting on DLP Agent version 15.1 MP1)	Yes	Yes
Safari 13	No	No	No	No	No	No	Yes
Google Chrome 41.0.x	Yes	Yes	No	No	No	Yes	Yes
Google Chrome 50	No	Yes	Yes	Yes	Yes	Yes	Yes
Google Chrome 51	Yes (on DLP Agent version 14.0.2)	Yes	Yes	Yes	Yes	Yes	Yes
Google Chrome 52	Yes (on DLP Agent version 14.0.2)	Yes	Yes	Yes	Yes	Yes	Yes
Google Chrome 53	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Google Chrome 55		Yes 14.5 MP1	Yes	Yes	Yes	Yes	Yes
Google Chrome 56	No	No	Yes	Yes	Yes	Yes	Yes
Google Chrome 57	No	No	Yes	Yes	Yes	Yes	Yes
Google Chrome 58	No	No	Yes (starting on DLP Agent version 14.6 MP1)	Yes	Yes	Yes	Yes

Software Version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Google Chrome 59	No	No	Yes (starting on DLP Agent version 14.6 MP1)	Yes	Yes	Yes	Yes
Google Chrome 60 through 69	No	No	Yes	Yes	Yes	Yes	Yes
Google Chrome 73	No	No	No	No	No	Yes	Yes
Google Chrome 74	No	No	No	No	No	Yes, on version 15.5 MP1	Yes
Google Chrome 75	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Google Chrome 76	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1, with	Yes
Google Chrome 77	No	No	No	Yes, on version 15.0 MP1	Yes, on version 15.1 MP2	Yes, on version 15.5 MP1	Yes
Google Chrome 78-81	No	No	No	No	Yes, on version 15.1 MP2	Yes, on version 15.5 MP2	Yes
Google Chrome 83-85	No	No	No	No	Yes	Yes	Yes

Table 39: Email

Software Version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Outlook 2011	No	Yes	Yes	Yes	Yes	Yes	No
Outlook 2016	No	No	Yes	Yes	Yes	Yes	Yes
Outlook 2019	No	No	No	No	Yes, on version 15.1 MP1	Yes	Yes

Table 40: Instant messaging

Software Version	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5	DLP 15.7
Cisco Jabber	No	Yes	Yes	Yes	Yes	Yes	Yes
Skype	No	Yes	Yes	Yes	Yes	Yes	Yes

Support for Monitoring Applications Protected by System Integrity Protection

The DLP Agent monitors applications that are protected by System Integrity Protection (SIP) on macOS 10.11, 10.12, 10.13, 10.14, and 10.15. You can find the latest macOS version support at Default SIP Monitoring.

Default SIP monitoring

The DLP Agent monitors macOS applications protected by System Integrity Protection (SIP). The table below lists the DLP Agent and macOS versions where SIP monitoring is supported for a given Symantec Data Loss Prevention release.

Table 41: SIP monitoring supported by default

DLP Agent version	SIP monitoring supported by default
14.5	macOS 10.11 through 10.11.4
14.6.x	macOS 10.11 through 10.11.5
15.0.x	macOS 10.11 through 10.11.5 macOS 10.12 through 10.12.5 macOS 10.13.2 through 10.13.4 (on MP1)
15.1.x	macOS 10.11 through 10.11.6 macOS 10.12 through 10.12.6 macOS 10.13 through 10.13.3 (through 10.13.6 on MP1)
15.5.x	macOS 10.11 through 10.11.6 macOS 10.12 through 10.12.6 macOS 10.13 through 10.13.6 macOS 10.14.0
15.7	macOS 10.11 through 10.11.6 macOS 10.12 through 10.12.6 macOS 10.13 through 10.13.6 macOS 10.14 through 10.15.2

Monitoring SIP-protected applications on updated macOS endpoints

If you plan to update the macOS to a version that exceeds the default supported version for a given DLP Agent version, you must update the agent configuration to continue monitoring applications protected by System Integrity Protection (SIP). If you do not update the agent configuration, the DLP Agent can no longer monitor these applications, and DLP Agent versions 14.6.x and 15.0.x display a **Critical** agent alert. The agent continues to monitor all other channels.

> **NOTE**
>
> For a list of the DLP Agent and macOS versions where SIP monitoring is supported by default, see Default SIP monitoring.

Steps to monitor SIP-protected applications on updated macOS endpoints.

Steps to monitor SIP-protected applications on updated macOS endpoints

Complete the following steps to monitor SIP-protected applications on updated macOS endpoints:

1. Log in to the Enforce Server administration console.
2. Go to **System > Agents > Agent Configuration** and click an agent configuration that is applied to the macOS agent.
3. Click the **Advanced agent settings** tab and locate the setting: Hooking.SIP_AGENT_OSX_VERSION_COMPATIBILITY.str.
4. Add the DLP Agent version and updated macOS version to the default value separated by a semicolon.

   macOS and DLP Agent version 15.x combinations list SIP monitoring support for macOS and DLP Agent version combinations. Refer to Monitoring macOS applications where SIP is enabled for version 14.x combinations. The table lists the value you enter to enable SIP monitor coverage. "Not supported" indicates that SIP monitoring is not supported for the macOS and DLP Agent version combination. "Supported" indicates that you are not required to enter a string to monitor SIP-protected application on the macOS/DLP Agent version.

5. Consider the following when adding strings to the Hooking.SIP_AGENT_OSX_VERSION_COMPATIBILITY.str setting:
   - Add new values using the default syntax: `DLPAgent-version:macOS-version`.
   - Add a value for each DLP Agent version (14.5 and greater) running on endpoints. For example, if you are running version 14.6 and 14.6 MP1 agents with macOS version 10.12.0, you enter a separate value for each agent version (14.6 and 14.6 MP1 agents). For this example scenario, you would enter `14.6.0:10.12.5;14.6.0100:10.12.5`.
   - Enter a DLP Agent version that exactly matches the version that displays on the Enforce Server administration console. Refer to the Agent Overview screen in the Enforce Server administration console to confirm the agent version.
   - Enter a macOS version equal to or greater than the macOS version running on endpoints. If you enter `14.6.0100:10.12.5`, macOS versions 10.12 through 10.12.5 are monitored on version 14.6 MP1 agents.
   - Add a value for each DLP Agent version (14.5 and greater) running on endpoints. For example, if you are running DLP Agent version 14.6 (on macOS 10.12.0 endpoints) and 14.6 MP1 (on macOS endpoints up to version 10.12.5) in your environment, you enter the following: `14.6.0:10.12.0;14.6.0100:10.12.5`.

     NOTE

     DLP Endpoint Agent hot fixes are cumulative for both Mac and Windows machines. Thus, if you have applied a subsequent hot fix for your Mac Agent, you will need to update the SIP settings accordingly. For example, the latest Public Hotfix for Mac Agents is 15.0.0107 - and it includes the hot fix for the Kernel Panic. Thus, the correct SIP settings for Macs running the latest hotfix for their respective releases is: `15.0.0107:10.11.6;15.0.0107:10.12.6;15.0.0107:10.13.4`.
6. Save your changes to apply the setting. After saving changes, the agent begins monitoring SIP-protected applications. For version 14.6.x and 15.0.x agents, saving also updates the agent alert status from **Critical** to **OK**.

Table 42: macOS and DLP Agent version 15.x combinations

macOS version	DLP version 15.1	DLP version 15.5	DLP version 15.7
10.11.3	Supported	Supported	Supported
10.11.4	Supported	Supported	Supported
10.11.5	Supported	Supported	Supported
10.11.6	Supported	Supported	Supported
10.12.0	Supported	Supported	Supported
10.12.1	Supported	Supported	Supported
10.12.2	Supported	Supported	Supported
10.12.3	Supported	Supported	Supported
10.12.4	Supported	Supported	Supported
10.12.5	Supported	Supported	Supported
10.12.6	Supported	Supported	Supported
10.13.0	Supported	Supported	Supported
10.13.1	Supported	Supported	Supported
10.13.2	Supported	Supported	Supported
10.13.3	Supported	Supported	Supported
10.13.4	• For 15.1 enter: `15.1.0:10.13.4` • Supported on 15.1 MP1 and MP2	Supported	Supported

macOS version	DLP version 15.1	DLP version 15.5	DLP version 15.7
10.13.5	• For 15.1 enter: `15.1.0:10.13.5` • Supported on 15.1 MP1 and MP2	Supported	Supported
10.13.6	• For 15.1 enter: `15.1.0:10.13.6` • Supported on 15.1 MP1 and MP2	Supported	Supported
10.14	• For 15.1 enter: `15.1.0:10.14.0` • Supported on 15.1 MP1 and MP2	Supported	Supported
10.14.1	• Not supported on 15.1 and 15.1 MP2 • For 15.1 MP1 enter: `15.1.0100:10.14.1`	• For 15.5 enter: `15.5.0:10.14.1` • For 15.5 MP1 enter `15.5.0100:10.14.1` • For 15.5 MP2 enter `15.5.0:10.14.1`	Supported
10.14.2	• Not supported on 15.1 and 15.1 MP2 • For 15.1 MP1 enter: `15.1.0100:10.14.2`	• For 15.5 enter: `15.5.0:10.14.2` • For 15.5 MP1 enter `15.5.0100:10.14.2` • For 15.5 MP2 enter `15.5.0:10.14.2`	Supported
10.14.3	Not supported	• For 15.5 enter: `15.5.0:10.14.3` • For 15.5 MP1 enter `15.5.0100:10.14.3` • For 15.5 MP2 enter `15.5.0:10.14.3`	Supported
10.14.4	Not supported	• For 15.5 enter: `15.5.0:10.14.4` • For 15.5 MP1 enter `15.5.0100:10.14.4` • For 15.5 MP2 enter `15.5.0:10.14.4`	Supported
10.14.5	• Not supported for 15.1 • For 15.1 MP2 enter: `15.1.0200:10.14.5`	• Not supported for 15.5 • For 15.5 MP1 enter `15.1.0104:10.14.5` You must install the latest 15.5 MP1 Hotfix to use this string. • For 15.5 MP2 enter: `15.5.0204:10.14.5`	Supported

macOS version	DLP version 15.1	DLP version 15.5	DLP version 15.7
10.14.6	• Not supported for 15.1 • For 15.1 MP2 enter: `15.1.0200:10.14.6`	• Not supported for 15.5. • For 15.5 MP1 enter `15.5.0106:10.14.6` You must install the latest 15.5 MP1 Hotfix to use this string. • For 15.5 MP2 enter: `15.5.0204:10.14.6` You must install the latest 15.5 MP2 Hotfix to use this string.	Supported
10.15	• Not supported on 15.1 and 15.1 MP1 • For 15.1 MP2 enter: `15.1.0200:10.15.0`	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0204:10.15.0` You must install the latest 15.5 MP2 Hotfix to use this string.	Supported
10.15.1	• Not supported on 15.1 and 15.1 MP1 • For 15.1 MP2 enter: `15.1.0209:10.15.1` You must install the latest 15.1 MP2 Hotfix to use this string.	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0204:10.15.1` You must install the latest 15.5 MP2 Hotfix to use this string.	Supported
10.15.2	• Not supported on 15.1 and 15.1 MP1 • For 15.1 MP2 enter: `15.1.0209:10.15.2` You must install the latest 15.1 MP2 Hotfix to use this string.	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0204:10.15.2` You must install the latest 15.5 MP2 Hotfix to use this string.	Supported
10.15.3	Not supported	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0304:10.15.2` You must install the latest 15.5 MP2 Hotfix to use this string.	Supported
10.15.4	• Not supported on 15.1 and 15.1 MP1. • For 15.1 MP2 enter: `15.1.0212:10.15.4` You must install the latest 15.1 MP2 Hotfix to use this string.	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0210:10.15.4` You must install the latest 15.5 MP2 Hotfix to use this string.	Enter `15.7.0:10.15.4`
10.15.5	• Not supported on 15.1 and 15.1 MP1. • For 15.1 MP2 enter: `15.1.0215:10.15.5` You must install the latest 15.1 MP2 Hotfix to use this string.	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0213:10.15.5` You must install the latest 15.5 MP2 Hotfix to use this string.	• Not supported on 15.7. • For 15.7 MP1 enter: `15.7.0100:10.15.5`

macOS version	DLP version 15.1	DLP version 15.5	DLP version 15.7
10.15.6	• Not supported on 15.1 and 15.1 MP1. • For 15.1 MP2 enter: `15.1.0215:10.15.6` You must install the latest 15.1 MP2 Hotfix to use this string.	• Not supported on 15.5 and 15.5 MP1. • For 15.5 MP2 enter: `15.5.0213:10.15.6` You must install the latest 15.5 MP2 Hotfix to use this string.	• Not supported on 15.7. • For 15.7 MP1 enter: `15.7.0100:10.15.6`

Endpoint known issues

This table lists the Endpoint known issues in 15.7.

Table 43: Endpoint known issues in 15.7

Issue	Description	Workaround
4151955	On Windows endpoints, if a user attempts to upload multiple sensitive files to Firefox using drag and drop to a site that does not support drag and drop, then performs the same action with the same files to a site that supports drag and drop, block pop-ups display twice for each file and two incidents are logged for each upload attempt.	None.
4208190	On Windows endpoints, filters for HTTPS are not applied to files saved using a **Save As** operation from Microsoft Office applications to SharePoint or OneDrive.	Add * to the beginning and end of the HTTPs filter. For example, if the existing HTTPS filter is *-dav.box.com*, which correctly applies a filter to Internet Explorer and Firefox, add another filter to monitor **Save As** operations from Office apps: **dav.box.com**.
4248826	Users are unable to paste content to Internet Explorer from the Clipboard when Edge is monitored using the Application Monitoring feature.	None.
4248828	Opening a Microsoft Office file that contains sensitive data residing on a network share triggers an incident.	None.
4249161	Symantec Data Loss Prevention Endpoint Discover now supports the **Limit Incident Data Retention** response rule for eDAR scans on Microsoft Windows endpoints; however, you cannot use the **Limit Incident Data Retention** response rule in combination with any other response rule.	None.
4250243	If a user launches an application while logged on as another user (**Run as different user**) and attempts to upload sensitive information, an incident is generated as expected. However, no pop-up alert is displayed to the user, even if the response rule is configured to display a pop-up alert.	None.
4268115	If a user running macOS 10.15.4 saves a `.doc` file that contains sensitive data to a removable storage device, detection does not occur.	None.
4268116	If a user running macOS 10.15.4 uploads a sensitive file to Box using Safari, detection occurs, and a file with a zero byte size is uploaded to Box.	None.

Issue	Description	Workaround
4267712	If a user installs Firefox 74 for the first time with the DLP Agent running, URL filters do not work and Block and notify pop-ups display unknown for the URL when sensitive files are uploaded.	Complete the following to enable URL filters and URL information: 1. Uninstall Firefox 74. 2. Confirm that the DLP Agent is running on the endpoint and install Firefox 73. 3. Upgrade to Firefox 74.

Copyright Statement

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Symantec™

A Division of Broadcom