Symantec™ Data Loss Prevention Upgrade Guide for Windows

Version 14.5
Symantec Data Loss Prevention Upgrade Guide for Windows

Documentation version: 14.5b

Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

support.symantec.com

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

Contacting Technical Support

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

support.symantec.com

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

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

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

**Licensing and registration**

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


**Customer service**

Customer service information is available at the following URL:


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

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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare_apj@symantec.com">customercare_apj@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>
Preparing to upgrade Symantec Data Loss Prevention

This chapter includes the following topics:

- About preparing to upgrade Symantec Data Loss Prevention
- Symantec Data Loss Prevention upgrade phases
- Preparing the Oracle database for a Symantec Data Loss Prevention upgrade
- About the minimum system requirements for upgrading to the current release
- About upgrading installations with mixed operating systems
- Supported upgrade backward compatibility for agents and servers
- About the requirement for language pack upgrades
- Upgrade requirements and restrictions
- About choosing an upgrade method
- Preparing your system for the upgrade
- About external storage for incident attachments
- About upgrading the detection servers
- About detection server upgrade restrictions
About preparing to upgrade Symantec Data Loss Prevention

To review the new features for Symantec Data Loss Prevention 14.5, see the *What’s New and What’s Changed in Symantec Data Loss Prevention 14.5* document, available with the rest of your downloaded Symantec Data Loss Prevention product documentation.

All Symantec Data Loss Prevention upgrades must be performed incrementally from one major or minor release to the next. From Symantec Data Loss Prevention 12.x you can upgrade to version 14.0, then to version 14.x.

Symantec Data Loss Prevention 14.5 enables you to upgrade version 12.x detection servers in stages, while still using non-upgraded detection servers to monitor and prevent confidential data loss. To upgrade to version 14.5, you begin by upgrading the Enforce Server (assuming that your database is already running on Oracle 11.2.0.4 or 12c). The upgraded Enforce Server can communicate with version 12.x detection servers for the purpose of recording new incidents and preventing confidential data loss. You can schedule the remaining detection server upgrades for a time that minimizes service interruption, with certain restrictions.

See “Upgrade requirements and restrictions” on page 17.

Back up your database before any upgrade. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for more information. If you must upgrade your Oracle database, upgrade it before you upgrade to Symantec Data Loss Prevention 14.5.

Symantec Data Loss Prevention upgrade phases

An upgrade is performed in the phases described in the table *Symantec Data Loss Prevention upgrade phases*.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade your database to Oracle 11g (11.2.0.4). <strong>Note:</strong> Oracle 12c is also supported, but it is not distributed by Symantec. For details about running Symantec Data Loss Prevention on Oracle 12c, see the Oracle 12c Implementation Guide at <a href="http://www.symantec.com/docs/DOC9260">http://www.symantec.com/docs/DOC9260</a>.</td>
<td>Upgrade your database to ensure continued security fixes. See the <em>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</em>.</td>
</tr>
</tbody>
</table>
### Table 1-1  Symantec Data Loss Prevention upgrade phases (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2     | Review important information about the new release before starting the upgrade, including:  
- Known release issues.  
- Minimum system requirements.  
- Language pack requirements.  
- *What’s New and What’s Changed.* | See the *Symantec Data Loss Prevention 14.5 Release Notes* at [http://www.symantec.com/docs/DOC9255](http://www.symantec.com/docs/DOC9255) to learn about any known upgrade issues or issues with the current release of Symantec Data Loss Prevention.  
The *What’s New and What’s Changed* is included with the rest of the product documentation you downloaded from FileConnect.  
See “About the minimum system requirements for upgrading to the current release” on page 14.  
See “About the requirement for language pack upgrades” on page 17. |
| 3     | Prepare the system for upgrading: This preparation includes backing up the Oracle database and detection server data. If the upgrade fails you can use these backups to restore your system.  
- Run the upgrader data pre-checker tool to check your database for compatibility with the new release.  
  See “Using the upgrader data pre-checker tool” on page 12.  
- Back up the Oracle database and detection server data. If the upgrade fails you can use these backups to restore your system. | See “Preparing your system for the upgrade” on page 18. |
| 4     | Download and extract the version 14.5 software. | See “Downloading and extracting the upgrade software” on page 24. |
| 5     | Using the Upgrade Wizard, upgrade the Enforce Server and detection servers.  
If necessary, perform a local upgrade on any detection servers that were not upgraded using the Upgrade Wizard. | See “Performing an upgrade with the Upgrade Wizard” on page 27.  
See “Locally upgrading a detection server” on page 31. |
| 6     | Upgrade Symantec Data Loss Prevention Agents. | See “About Symantec Data Loss Prevention Agent upgrades” on page 34. |
| 7     | Upgrade any scanners. | See “Upgrading your scanners” on page 33. |
Table 1-1 Symantec Data Loss Prevention upgrade phases (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Complete the required and optional post-upgrade tasks.</td>
<td>See “Performing post-upgrade tasks” on page 54.</td>
</tr>
</tbody>
</table>

Preparing the Oracle database for a Symantec Data Loss Prevention upgrade

The following Oracle-related preparations must be made before you use the Upgrade Wizard to upgrade the Symantec Data Loss Prevention database schema for version 14.5:

- Run the upgrade data pre-checker tool to check your current database against the new constraints introduced in Symantec Data Loss Prevention 14.5. See “Using the upgrader data pre-checker tool” on page 12.
- Back up the Oracle database before you start the upgrade. You cannot recover from an unsuccessful upgrade without a backup of your Oracle database. For more information, see the Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide.

See “Preparing your system for the upgrade” on page 18.

Using the upgrader data pre-checker tool

The upgrader data pre-checker is a tool you can run on your Oracle database to check your existing data against new constraints introduced in Symantec Data Loss Prevention 14.5. This allows you to address any data issues related to the new constraints before you upgrade your system. Because the tool does not validate all of your data, your database may still have issues that need to be resolved before upgrade.

The upgrader data pre-checker tool creates a report of any violations of the new constraints in your database. The report is formatted as an HTML file. If the tool returns any constraint violations, send a copy of the HTML report to Symantec Technical Support for help resolving these issues before you upgrade your system to Symantec Data Loss Prevention 14.5.

Note: Because you must contact Symantec Technical Support to resolve any issues with your database before upgrading your system, Symantec recommends running the upgrader data pre-checker tool several days before you plan to upgrade.
The upgrader data pre-checker tool is available in the Upgrade folder in the Platform ZIP file that contains your Symantec Data Loss Prevention software:

- Symantec_DLP_14.5_Platform_Win-IN.zip

Within this ZIP file, locate the Upgrader_Data_Prechecker_14_5_0_0.zip file and extract it as the Oracle user (the user with SQL*Plus privileges) to the host computer for your Oracle installation, or to another computer that has access to your Oracle host computer: DLP/14.5/Upgrade_14.0_to_14.5/Upgrader_Data_Prechecker.

When necessary, Symantec will post an updated version of the tool to the Symantec Support Center here: [http://www.symantec.com/docs/TECH234801](http://www.symantec.com/docs/TECH234801). To be notified of any updates to the tool, subscribe to this article.

To run the upgrader data pre-checker tool

1. On the Oracle host computer or other computer with access to your Oracle host computer, log on as the Oracle user.
2. Open a command prompt and navigate to the Upgrader_Data_Prechecker folder you extracted from your Platform ZIP file.
3. Log in to SQL*Plus as the Symantec Data Loss Prevention Oracle user:

   sqlplus protect/protect@protect

4. Run the run.sql script:

   @run.sql

5. The script runs for a few minutes and generates the report: Upgrader_Data_Prechecker.html.
6. Open the report in a web browser to view the results, then take one of the following actions:

   - If the report lists any violated constraints, contact Symantec Technical Support at [www.symantec.com/business/support](http://www.symantec.com/business/support). Your support contact will ask you to email the Upgrader_Data_Prechecker.html file to assist in resolving any violated constraint issues in your database before you upgrade your system.
   - If the report does not list any violated constraints, proceed with the upgrade process.
About the minimum system requirements for upgrading to the current release

The free disk space requirements for upgrading an existing Symantec Data Loss Prevention installation depend on the server type:

- Enforce Server single-, two-, or three-tier installation: 50 GB (for small/medium enterprise) to 100 GB (for large/very large enterprise) of free disk space on the volume where the server is installed.
- Detection server: 750 MB of free disk space on the volume where the server is installed.

Note: These numbers refer to the free disk space needed for the upgrade process, not the disk space that is required for server operation. For server disk space, operating system, and other requirements, see the Symantec Data Loss Prevention System Requirements and Compatibility Guide.

See “About preparing to upgrade Symantec Data Loss Prevention” on page 10.

About upgrading installations with mixed operating systems

Some Symantec Data Loss Prevention installations have servers running on both the Linux and Windows operating systems. The Upgrade Wizard provided with Symantec Data Loss Prevention 14.5 can upgrade detection servers that are running on both operating systems.

See “Locally upgrading a detection server” on page 31.

Supported upgrade backward compatibility for agents and servers

As you upgrade your Endpoint protection, you may have different components of the suite on different versions. During the upgrade process, you may have an Enforce Server on version 14, Endpoint Servers on version 12.x, and agents on version 12.x. The following table describes the scenarios where multi-version servers and agents are possible. The described scenarios are only possible during the upgrade process. The scenarios assume that you have already upgraded your Enforce Server to version 14. You cannot upgrade either your Endpoint Servers or your agents before upgrading your Enforce Server.
If your agents and Endpoint Servers are on versions earlier than 14.0, do not restart the Endpoint Server. If you restart the Endpoint Server when it is not on the current version, all policy and all configuration information is lost.

If all of the policy and the configuration information is lost, you must upgrade the Endpoint Server and the agents to the most current version. Upgrade Endpoint Servers to version 14.5. Upgrade agents to version 12.0 (at a minimum) or 14.5. When you upgrade to the current version, first upgrade the Endpoint Server then upgrade agents. For example, if you have a version 11.6.3 Enforce Server, and version 10.0 Endpoint Server and agents, you upgrade the Endpoint Server to version 12.0 and then upgrade the agents to version 12.0. You can then upgrade from version 12.0 to version 14.0, and then to 14.5. Upgrading the Endpoint Server first ensures that your servers and agents are in a supported configuration.

The most stable configuration is for all Enforce Servers, Endpoint Servers, and agents to be on version 14.5. Ideally, you will only be on one of the following backward-compatible scenarios for a limited time as you upgrade all servers and agents to version 14.5.

Table 1-2 Supported backward compatibility for agent upgrades

<table>
<thead>
<tr>
<th>Enforce Server version</th>
<th>Endpoint Server version</th>
<th>Symantec DLP Agent version</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.5</td>
<td>14.5</td>
<td>14.5</td>
<td>Best option for backward compatibility. All incidents are sent to the Enforce Server. Policy and configuration updates can be sent to the Endpoint Servers and agents.</td>
</tr>
<tr>
<td>14.5</td>
<td>14.5</td>
<td>14.0 12.5.x 12.0.x</td>
<td>Agents and the Endpoint Server send incidents based on existing policies that were configured before the upgrade. Policies and configuration settings can be sent to Endpoint Servers and agents.</td>
</tr>
</tbody>
</table>
## Table 1-2: Supported backward compatibility for agent upgrades (continued)

<table>
<thead>
<tr>
<th>Enforce Server version</th>
<th>Endpoint Server version</th>
<th>Symantec DLP Agent version</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.5</td>
<td>14.0</td>
<td>14.0</td>
<td>Agents and the Endpoint Server send incidents based on existing policies that were configured before the upgrade. Policies and configuration settings cannot be sent to Endpoint Servers and agents. If the Endpoint Server restarts, all policies and configurations are lost. Incidents are no longer sent to the server.</td>
</tr>
<tr>
<td></td>
<td>12.5.x</td>
<td>12.5.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12.0.x</td>
<td></td>
</tr>
<tr>
<td>14.5</td>
<td>12.0.x</td>
<td>12.0.x</td>
<td>Agents and the Endpoint Server send incidents based on existing policies that were configured before the upgrade. Policies and configuration settings cannot be sent to Endpoint Servers and agents. If the Endpoint Server restarts, all policies and configurations are lost. Incidents are no longer sent to the server.</td>
</tr>
</tbody>
</table>
About the requirement for language pack upgrades

Symantec Data Loss Prevention requires version-specific language packs. The upgrade process removes all older language packs and rolls the user interface back to the English-language default. After the upgrade, you must download and add new versions of each language pack as needed. See the Symantec Data Loss Prevention Administration Guide for information about acquiring and adding updated language packs.

See “About preparing to upgrade Symantec Data Loss Prevention” on page 10.

Upgrade requirements and restrictions

The following are requirements for performing an upgrade, and known issues that can occur when you upgrade Symantec Data Loss Prevention:

- You must stop all Network Discover scans before you upgrade the Enforce Server to version 14.5. You cannot restart Network Discover scans until at least one Network Discover detection server has been upgraded to version 14.5.

- If a version or 12.x detection server stops (shuts down) after you have upgraded the Enforce Server to version 14.5, you must upgrade that detection server to version 14.5 before it can restart.

- After you upgrade the Enforce Server to version 14.5, any configuration changes that you make have no effect on version 12.x detection servers.

- After you complete the upgrade, do not modify the host name or IP address of a detection server to point to a different detection server. Detection servers use the original configured IP address or host name to maintain and report server-level statistics.

- Restart the Vontu Monitor Controller service to verify the upgraded detection server versions in the Enforce Server administration console.

See “About preparing to upgrade Symantec Data Loss Prevention” on page 10.

About choosing an upgrade method

You can upgrade a system from one version of Symantec Data Loss Prevention to another in two ways:

- Through the Upgrade Wizard, which you access through the Enforce Server. The Upgrade Wizard provides the easiest and most efficient way to upgrade Symantec Data Loss Prevention.

See “Performing an upgrade with the Upgrade Wizard” on page 27.
Locally (in other words, manually) on individual detection servers. You can upgrade a detection server manually in the following cases:

- If a detection server failed to receive its patch files.
- If a detection server was disconnected from the network.
- If the Symantec Data Loss Prevention services of a detection server were shut down at the time you upgraded the Enforce Server, using the Upgrade Wizard.

See “About preparing to upgrade Symantec Data Loss Prevention” on page 10.

Preparing your system for the upgrade

Before upgrading to the current version of Symantec Data Loss Prevention, make sure that your system meets the upgrade requirements. These requirements as described in the following topics:

- See “Upgrade requirements and restrictions” on page 17.
- See “About external storage for incident attachments” on page 18.
- See “Preparing the Oracle database for a Symantec Data Loss Prevention upgrade” on page 12.
- See “About upgrading the detection servers” on page 19.

Make sure that you have also reviewed and acted on the information in the following topic:

- See “About the minimum system requirements for upgrading to the current release” on page 14.

About external storage for incident attachments

You can store incident attachments such as email messages or documents on a file system rather than in the Symantec Data Loss Prevention database. Storing incident attachments externally saves a great deal of space in your database, providing you with a more cost-effective storage solution.

You can store incident attachments either in a directory on the Enforce Server host computer, or on an stand-alone computer. You can use any file system you choose. Symantec recommends that you work with your data storage administrator to set up an appropriate directory for incident attachment storage.

To set up an external storage directory, Symantec recommend these best practices:
If you choose to store your incident attachments on the Enforce Server host computer, do not place your storage directory under the /SymantecDLP/ folder.

If you choose to store incident attachments on a computer other than your Enforce Server host computer, take the following steps:

- Ensure that both the external storage server and the Enforce Server are in the same domain.
- Create a "protect" user with the same password as your Enforce Server "protect" user to use with your external storage directory.
- If you are using a Linux system for external storage, change the owner of the external storage directory to the external storage "protect" user.
- If you are using a Microsoft Windows system for external storage, share the directory with Read/Write permissions with the external storage "protect" user.

After you have set up your storage location you can enable external storage for incident attachments in the Upgrade Wizard. After you have upgraded your system to Symantec Data Loss Prevention 14.5, all new incident attachments will be stored in the external storage directory. In addition, a migration process runs in the background to move your existing incident attachments from the database to your external storage directory. Incident attachments in the external storage directory cannot be migrated back to the database. Incident attachments stored in the external storage directory are encrypted and can only be accessed from the Enforce Server administration console.

The incident deletion process deletes incident attachments in your external storage directory after it deletes the associated incident data from your database. You do not need to take any special action to delete incidents from the external storage directory.

About upgrading the detection servers

Symantec Data Loss Prevention version 12.5 introduced a new framework for automatically distributing upgrade packages to detection servers before or during the upgrade process. This new approach to package distribution shortens and simplifies the upgrade process. To begin this automated distribution process, download and extract the upgrade software. The Enforce Server automatically detects the upgrade packages and begins distributing the patches to your detection servers. When you choose to upgrade your system, you can view the patch distribution status in the Upgrade Wizard.
If you do not want Symantec Data Loss Prevention to automatically distribute your detection server upgrade packages, you can disable the automatic distribution feature.

See “Downloading and extracting the upgrade software” on page 24.

Note: Only detection servers running Symantec Data Loss Prevention version 12.5 or later can receive the automatically distributed patches. Detection servers running Symantec Data Loss Prevention version 12.0.x receive their patch files during the upgrade process.

Prepare for upgrading your detection servers by reviewing the following prerequisites:

- Make sure that the Symantec Data Loss Prevention services on each detection server are running before you start the upgrade. See “Verifying that the Enforce Server and the detection servers are running” on page 25.

- Upgrade your detection servers to Symantec Data Loss Prevention version 14.0 or later. Version 12.x or older detection servers are not compatible with the version 14.5 Enforce Server.

- Upgrade your Endpoint Servers to version 14.5 to ensure that your DLP Agents can receive updated policies and configurations.

- Before performing an upgrade using the Upgrade Wizard, verify that all the detection servers to be upgraded are connected. If a detection server is disconnected when you upgrade the Enforce Server using the Upgrade Wizard, you can upgrade it later by re-running the Upgrade Wizard, or by performing a local (manual) upgrade.

- Before locally upgrading any detection server, you must run the Upgrade Wizard to upgrade the Enforce Server.

- If you have servers with low-bandwidth connections, upgrade them locally.

- Make sure that all Network Discover scans are halted before starting the upgrade.

See “Preparing your system for the upgrade” on page 18.

About detection server upgrade restrictions

Only detection servers on version 14.0 or later can receive the automatically distributed upgrade packages.

You cannot upgrade a detection server from a version that is older than 14.0 using the Symantec Data Loss Prevention 14.5 Upgrade Wizard. If you have a detection
server that is older than 14.0, first perform a local upgrade of that detection server to 14.0. You can then use the Upgrade Wizard to upgrade the detection server to 14.5.

See “Verifying that the Enforce Server and the detection servers are running” on page 25.

See “Preparing your system for the upgrade” on page 18.
Upgrading Symantec Data Loss Prevention to a new release

This chapter includes the following topics:

- Upgrading Symantec Data Loss Prevention
- Downloading and extracting the upgrade software
- Setting the Upgrade Wizard port number
- Verifying that the Enforce Server and the detection servers are running
- Launching the Upgrade Wizard on the Enforce Server
- Performing an upgrade with the Upgrade Wizard
- Locally upgrading a detection server
- Applying the updated configuration to Endpoint Prevent servers
- Upgrading your scanners
- Upgrading Endpoint Prevent group directory connections

Upgrading Symantec Data Loss Prevention

After preparing your system for the upgrade, you are ready to perform the upgrade itself. The following table describes the high-level steps that are involved in upgrading Symantec Data Loss Prevention. Each step is described in more detail elsewhere in this chapter, as indicated.
Note: If you are upgrading your system and you have deployed Exact Data Matching (EDM) profiles and policies, there is a specific upgrade path you need to perform so that your profiles and policies update properly.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download and extract the upgrade software.</td>
<td>See &quot;Downloading and extracting the upgrade software&quot; on page 24.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Specify the Upgrade Wizard port number.</td>
<td>See &quot;Setting the Upgrade Wizard port number&quot; on page 24.</td>
</tr>
<tr>
<td>3</td>
<td>Make sure that the Enforce Server and the detection servers are running.</td>
<td>See &quot;Verifying that the Enforce Server and the detection servers are running&quot; on page 25.</td>
</tr>
<tr>
<td>4</td>
<td>Close all files and folders in your SymantecDLP directory.</td>
<td>Ensure that all folders and files in your SymantecDLP directory are closed and unlocked. The upgrader requires access to all SymantecDLP folders and files during the upgrade process.</td>
</tr>
<tr>
<td>6</td>
<td>Perform the upgrade with the Upgrade Wizard.</td>
<td>See “Performing an upgrade with the Upgrade Wizard” on page 26.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) Apply the updated agent configuration to Endpoint Prevent detection servers.</td>
<td>See “Applying the updated configuration to Endpoint Prevent detection servers” on page 32.</td>
</tr>
<tr>
<td>8</td>
<td>(Optional) Update Endpoint Symantec DLP Agents.</td>
<td>See &quot;About Symantec Data Loss Prevention Agent upgrades&quot; on page 34.</td>
</tr>
<tr>
<td>9</td>
<td>(Optional) Update any scanners.</td>
<td>See “Upgrading your scanners” on page 33.</td>
</tr>
<tr>
<td>10</td>
<td>Upgrade WinPcap (Network Monitor deployments only).</td>
<td></td>
</tr>
</tbody>
</table>
Downloading and extracting the upgrade software

To download the upgrade software

◆ Copy the ZIP files to the computer from where you intend to perform the upgrade. That computer must have a reliable network connection to the Enforce Server.

The files within this ZIP file must be extracted into a directory on a system that is accessible to you. The root directory into which the ZIP files are extracted is referred to as the `DLPDownloadHome` directory.

To extract the ZIP files

1. **Extract the contents of the Symantec_DLP_14.5_Platform_Win-IN.zip file.**
   
   Among other items, the ZIP file contains an Upgrade_14.0_to_14.5 folder, which includes an upgrade JAR (Java archive) file that is required later when you run the Upgrade Wizard.

2. **Extract the contents of the Symantec_DLP_14.5_Agent_Win-IN.zip file.**
   
   Among other items, the ZIP file contains the `DLPDownloadHome\DLP\14.5\Endpoint\Win\x64\AgentInstall64.msi` file for 64-bit endpoints and the `DLPDownloadHome\DLP\14.5\Endpoint\Win\x86\AgentInstall.msi` file for 32-bit endpoints. You use these files when you generate the agent installation package.

3. **Extract the contents of the Symantec_DLP_14.5_Agent_Mac-IN.zip file.**
   
   Among other items, the ZIP file contains the `DLPDownloadHome\14.5\Endpoint\Mac\x86_64\AgentInstall.pkg` file. You use this file when you generate the agent installation package.

4. Note where you saved the upgrade JAR, MSI, and PKG files so you can quickly find them later.

See “Setting the Upgrade Wizard port number” on page 24.

See “Symantec Data Loss Prevention upgrade phases” on page 10.

Setting the Upgrade Wizard port number

The Upgrade Wizard has its own default port number, which is 8300. If your organization reserves that port for another purpose, you can reconfigure the Upgrade Wizard to use another port.
To set the Upgrade Wizard port number

1. Open the following file in a text editor:

`SymanetcDLP\Protect\Manager.properties`

2. Add the following line to the file:

```properties
update.wizard.port=port
```

Where `port` equals the number of the port you want the Upgrade Wizard to use.

Enter a unique port number. Other applications on the Enforce Server host cannot use the same port. Verify that firewalls do not block the port number you enter. If firewalls block the port number you cannot access the Upgrade Wizard from a different computer than the Enforce Server host.

For example, the following line configures the Upgrade Wizard to use port 5555:

```properties
update.wizard.port=5555
```

See “Verifying that the Enforce Server and the detection servers are running” on page 25.

See “Upgrading Symantec Data Loss Prevention” on page 22.

Verifying that the Enforce Server and the detection servers are running

Verify that the Enforce Server is running.

Check that all of the detection servers to be upgraded using the Upgrade Wizard are running the appropriate Symantec Data Loss Prevention services.

See “About Symantec Data Loss Prevention services” on page 57.

Although it is easier to upgrade all the servers at the same time using the Upgrade Wizard, you can upgrade individual detection servers, if needed. If a detection server is disconnected when you first run the Upgrade Wizard, you can re-run the Upgrade Wizard to upgrade the server, or you can perform a local server upgrade.

To ensure that the detection servers are running

1. Log on to the Enforce Server.

2. Go to **System > Servers and Detectors > Overview** and check that the Symantec Data Loss Prevention servers are running.

Launching the Upgrade Wizard on the Enforce Server

Before launching the Upgrade Wizard, review the following prerequisites and restrictions:

- Make sure that the JAR file you extracted earlier when you performed the upgrade prerequisite steps is available. See “Downloading and extracting the upgrade software” on page 24.
- If your installation uses FIPS encryption, your browser will not be able to redirect from the Enforce Server administration console to the Upgrade Wizard user interface. In this case, you must manually browse to https://Enforce_server:8300. (If you have changed the Upgrade Wizard port number, use that port number in the URL.)
- Clear your browser cache before upgrading the Enforce Server.
- Stop all DLP Endpoint Discover scans.
- Close all files and folders in your \SymantecDLP\ directory.

To launch the Upgrade Wizard on the Enforce Server

1. Ensure that all detection servers are running and are connected to the Enforce Server. See “About Symantec Data Loss Prevention services” on page 57.
2. Log on to your Enforce Server administration console.
3. Go to System > Servers and Detectors > Overview.
4. Click Upgrade.

The Upgrade System pop-up window appears.
From the directory that includes that JAR file, select the file and click Open.

The name of the file is 14.5_Upgrader_Windows.jar.

Click Launch Upgrade.

It may take several minutes for the Symantec Data Loss Prevention Upgrader Login panel to appear.

If the Enforce Server returns an error or times out, you must correct the problem before continuing.

See “About troubleshooting Symantec Data Loss Prevention upgrade problems” on page 62.

If no error occurs, the Symantec Data Loss Prevention Upgrader Login panel appears and you are ready to continue the upgrade. See “Performing an upgrade with the Upgrade Wizard” on page 27.

See “Symantec Data Loss Prevention upgrade phases” on page 10.

Performing an upgrade with the Upgrade Wizard

Should you encounter an error at any point during the upgrade, examine the log files.

To resolve errors

1. On the page where you encountered the error, click the Log Files link.

2. Try to resolve the error, and then launch the Upgrade Wizard again.

These procedures assume that you have already launched the Upgrade Wizard.


To upgrade the Enforce Server

1. On the Symantec Data Loss Prevention Upgrader Login panel, enter the Administrator user name and password, and then click logon.

   The License Agreement panel appears.

2. Click Accept.

   The System Check panel appears. When you click Next, the Upgrade Wizard verifies that you have the minimum software version level required to upgrade to the current release version.

3. Click Next.

   One of the following two outcomes results:
   - If the check was successful, the System Check Succeeded panel appears.
If at any point you see a message box stating that the upgrade has failed, click **Cancel**. Fix the reported problem that is shown in the panel. After fixing the problem, log on to Enforce, and launch the upgrade again.

4 From the **System Check Succeeded** panel, click **Next**.

The **Disable automatic distribution of detection server upgrade packages** page appears.

5 Select **Automatically distribute the detection server upgrade packages** if you want Symantec Data Loss Prevention to distribute your detection server upgrade packages automatically.

If you want to manually upgrade your detection servers, select **Manually upgrade detection servers**. Symantec Data Loss Prevention creates an upgrade package labeled `DetectionServerPatch14.5.0.0_1` in your updates directory which you can copy to the `c:\SymantecDLP\Protect\updates\DetectionUpgradePackages` directory of the Enforce Server and each detection server manually. Before you copy the upgrade packages to each detection server, stop the `VontuMonitorController` process on each detection server. After distributing the upgrade packages, you can use the Upgrade Wizard to complete the detection server upgrade process.

See “Locally upgrading a detection server” on page 31.

6 Click **Next**.

If you selected automatic detection server package distribution, the **Detection Server Upgrade Package Distribution Status** page appears. This page displays the status of the package distribution process. When the packages have been distributed, proceed to the next step.

7 Click **Next**.

The **Welcome to Symantec Data Loss Prevention Upgrader** panel appears.

A prompt warns you that any language packs you have installed from a previous version of Symantec Data Loss Prevention will be deleted. You must install new language packs for the current version of Symantec Data Loss Prevention later in the upgrade process.

8 Click **Next**.

The **Pre-check** panel appears and the Upgrade Wizard begins performing pre-upgrade tasks. The tasks include extracting necessary upgrade files and stopping Symantec Data Loss Prevention services.

9 Click **Next** after the pre-check tasks complete.
10 From the **Upgrade Enforce Server** panel, click **Next**.

The wizard creates a compressed file, called `SymantecDLPEnforceBackup_previousVersion.zip`, that contains all the files in your file system. It puts the file in a new update directory (`c:\SymantecDLP\Protect\updates\SymantecDLPEnforceBackup`). Then it installs new ones.

This step also upgrades the Symantec Data Loss Prevention schema on the Oracle database.

When the process has finished successfully, the following message appears:

*Done upgrading Enforce software.*

If an error occurs, a message to that effect appears. Consult the logs for information, correct the problem, and launch the upgrade again.

---

**Note:** If you launch the Upgrade Wizard again to upgrade the remaining detection servers, the utility does not repeat the Enforce Server upgrade.

11 Click **Next** after the Enforce upgrade completes.

The **Enable external storage for incident attachments** panel appears.

12 To enable external storage for incident attachments, select **Enable external storage for incident attachments** and enter or browse to the path of your **External Storage Directory**.

---

**Note:** If you enabled external storage for incident attachments in your previous version of Symantec Data Loss Prevention, ensure that you select **Enable external storage for incident attachments** and enter the path to your existing external storage directory.

See “About external storage for incident attachments” on page 18.

13 Click **Next**.

The **Enable Symantec DLP Supportability Telemetry** panel appears.

14 If you plan to share system information with Symantec, perform the following steps:

- Select **Participate in Supportability Telemetry Program**.
- Select **This DLP instance is a production system** to indicate your system is in production or **This DLP instance is a test system** to indicate your system is in test.
Enter your company name in the **Company Name** field.

15 Click **Next**.

The **Upgrade Detection Servers** panel appears.

16 After the detection server upgrade packages have been distributed automatically or manually, select the detection servers you want to upgrade then click **Upgrade**.

The wizard creates a compressed file, called `SymantecDLPDetectionBackup_previousVersion.zip`. This compressed file contains all of the files in your file system. It puts the compressed file in a new update directory `\SymantecDLP\Protect\updates\SymantecDLPDetectionBackup`. Then it installs new ones.

After the wizard upgrades the detection servers you selected, green checkmarks appear next to those servers listed in the **Upgrade Status** column of the panel.

If you experienced network connectivity problems between your Enforce Server and any detection server, you can locally upgrade those servers later. You can also run the Upgrade Wizard again.

See “Locally upgrading a detection server” on page 31.

---

**Note:** When you run the Upgrade Wizard again, it does not upgrade the Enforce Server again.

You must upgrade the Enforce Server before trying to upgrade your detection servers. Otherwise, you receive an error message in the system events report and the upgrade does not proceed.

Upgrade all detection servers to the same version as the newly upgraded Enforce Server to ensure compatibility. See “About upgrading the detection servers” on page 19.

17 Click **Next**.

The **Success** panel appears and prompts you to also upgrade your system endpoints.

18 Click **Finish**.

The **Symantec Data Loss Prevention Login** panel for Enforce Server appears.
19 If your Symantec Data Loss Prevention deployment uses the Veritas Cluster Server (VCS) high-availability solution, run the following script on each Enforce Server node:

\texttt{vcs\_upgrade.bat <SymantecDLP> <system user name>}

Where \texttt{<SymantecDLP>} is the directory where Symantec Data Loss Prevention is installed on the Enforce Server node and \texttt{<system user name>} is the DLP system user.

20 Log on to the Enforce Server.

The Enforce Server administration console appears.

21 Clear your browser cache to ensure that the initial page does not appear blank or as a previous version.

22 To verify that all of your Symantec Data Loss Prevention products are licensed for the current release, navigate to \texttt{System > Settings > General}.

If necessary, you can enter additional license files by clicking \texttt{Configure} on this page.

For more information, see the \textit{Symantec Data Loss Prevention Administration Guide}.

To verify the upgrade, review that your server version numbers are correct. Go to \texttt{System > Servers and Detectors > Overview} and click Enforce Server or a detection server.

\underline{Note:} The new version numbers for the upgraded detection servers do not display in the Enforce Server administration console until the Vontu Monitor Controller service has been restarted. The service does not start until the upgrade is complete.

Alternatively, on the Enforce Server, go to \texttt{\SymantecDLP\Protect} and check \texttt{Manager.ver}. To check on the detection server, go to the same directory and check \texttt{Monitor.ver}.

See “About Symantec Data Loss Prevention Agent upgrades” on page 34.
See “Symantec Data Loss Prevention upgrade phases” on page 10.

\textbf{Locally upgrading a detection server}

You can locally upgrade a detection server if it was disconnected from the network or its Vontu services were shut down at the time you upgraded the Enforce Server.
Upgrade the Enforce Server before performing local upgrades on detection servers.

To locally upgrade a detection server

1. Open the \SymantecDLP\Protect\updates directory on the detection server.

2. If it does not already exist, create a directory within \SymantecDLP\Protect\updates named detectionupgrade14.5. The directory name cannot contain spaces.

3. Copy the 14_5_WindowsDetectionUpgradePackage.jar file from the Enforce Server to the \SymantecDLP\Protect\updates\detectionupgrade14.5 directory on the detection server.

   If you manually uploaded the upgrade JAR to the Enforce Server, the required JAR file is located in \SymantecDLP\Protect\updates\enforceupgrade14.5.

   If you automatically uploaded the file, it is placed in \SymantecDLP\Protect\updates\update-id-x where x is a number based on the time the last upgrade was performed. Use the directory with the most recent modification time.

4. Extract the contents of the JAR file into the detectionupgrade14.5 directory. (You can use WinZip or WinRAR to extract the contents of the JAR file.)

   Make sure the files extract to the correct directory. The start_local_upgrade.bat file must be in the \SymantecDLP\Protect\updates\detectionupgrade14.5 directory before you can run it successfully.

5. Run the file named start_local_upgrade.bat as an Administrator.

6. Follow the options as they appear on the panel. Make sure that the destination directory is set to the detectionupgrade14.5 directory.

See “Symantec Data Loss Prevention upgrade phases” on page 10.

Applying the updated configuration to Endpoint Prevent servers

The upgrade process updates existing Endpoint Prevent agent configurations with new settings. After you complete the upgrade, the Enforce Server administration console reports that existing Endpoint Servers use an outdated configuration. Follow this procedure to apply the updated agent configuration to your Endpoint Servers.
To apply the updated configuration to Endpoint Prevent servers

1. Log on to the Enforce Server administration console using the Administrator account.
2. Select System > Agents > Agent Configuration.
3. Select Apply Configuration.
4. Select all available configurations, and then click Apply and Update.
5. Click Done.

Upgrading your scanners

If you have any version 14.0 or earlier scanners, you should upgrade them to Symantec Data Loss Prevention version 14.5 scanners. To upgrade a scanner, remove the older software and then install the Symantec Data Loss Prevention 14.5 scanner.

See the Symantec Data Loss Prevention Administration Guide for information on adding and removing scanners.

See “Symantec Data Loss Prevention upgrade phases” on page 10.

Upgrading Endpoint Prevent group directory connections

Symantec Data Loss Prevention provides server-side group-based policies, which require an index for each group directory connection that you use. If you have existing Endpoint Prevent group directories from a previous Symantec Data Loss Prevention version, you must create indexes and configure the indexing schedule for those group directories before associated group-based policies can be applied to detection servers.

See the Symantec Data Loss Prevention System Administration Guide for information about creating group directory connections and scheduling directory server indexing.
Upgrading Symantec DLP Agents

This chapter includes the following topics:

- About Symantec Data Loss Prevention Agent upgrades

About Symantec Data Loss Prevention Agent upgrades

You can upgrade DLP Agents from one version to another by using a systems management software, or you can update the agents manually. Manual upgrades are not recommended for large deployments. You can upgrade DLP Agents as a group if you upgrade using systems management software. If you upgrade the agents manually, you must upgrade each agent individually.

Note: You cannot run a version 11.x DLP Agent with a 14.5 Endpoint Server. Endpoint Servers are backward-compatible with a DLP Agent for one full release. For example, a version 14.5 Endpoint Server and a version 12.x DLP Agent are compatible.

Symantec recommends installing antivirus software on your endpoints. However, antivirus software may interrupt the DLP Agent upgrade if antivirus scans are being performed on agent installation directories. Therefore, pause antivirus scans on agent installation directories during the upgrade process.

After you upgrade agents to the latest version, each agent must reconnect to the Endpoint Server before detection resumes. The upgrade process deletes all stored policy configurations from the agents. After the agents reconnect to an Endpoint Server, the agents download the relevant policies.

The following table provides a general overview of the upgrade process:
### Table 3-1  Upgrade process for Symantec DLP Agents

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create the Symantec Data Loss Prevention Agent installation package.</td>
<td>You create the agent installation package using the Enforce Server administration console. This package contains a BAT file you use to upgrade Windows agents and a PKG file you use to upgrade the Mac agents.  See “About secure communications between DLP Agents and Endpoint Servers” on page 36.</td>
</tr>
<tr>
<td>2</td>
<td>Bundle the Mac agent installation files if you plan to upgrade Mac agents.</td>
<td>See “Process to upgrade the DLP Agent on Mac” on page 47.</td>
</tr>
<tr>
<td>3</td>
<td>Install the upgrade package on endpoints.</td>
<td>Choose one of the following upgrade methods:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Upgrade the DLP Agent by using silent upgrades.  See “Upgrading the Windows agent silently” on page 44.  See “Upgrading DLP Agents on Mac endpoints silently” on page 51.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Upgrade the DLP Agent manually.  See “Upgrading the Windows agent manually” on page 43.  See “Upgrading the DLP Agent for Mac manually” on page 50.</td>
</tr>
</tbody>
</table>
About secure communications between DLP Agents and Endpoint Servers

Symantec Data Loss Prevention supports bidirectional authentication and secure communications between DLP Agents and Endpoint Servers using SSL certificates and public-key encryption.

Symantec Data Loss Prevention generates a self-signed certificate authority (CA) certificate on installation or upgrade. The DLP Agent initiates connections to one of the Endpoint Servers or load balancer servers and authenticates the server certificate. All certificates used for agent to server communications are signed by the self-signed CA.

See “Working with endpoint certificates” on page 40.

Symantec Data Loss Prevention automatically generates the SSL certificates and keys needed for authentication and secure communications between DLP Agents and Endpoint Servers. You use the Enforce Server administration console to generate the agent certificate and keys. The system packages the agent certificates and keys with the agent installer for deployment of DLP Agents. The certificates and keys are generated for the agent during installation.

See “Generating agent installation packages” on page 36.

Generating agent installation packages

You use the System > Agents > Agent Packaging screen to generate the installation package for DLP Agents.

See “About secure communications between DLP Agents and Endpoint Servers” on page 36.

The packaging process creates a ZIP file that contains the agent installer, SSL certificate and keys, and installation scripts to install DLP Agents. You generate a single agent installation package for each endpoint platform where you want to deploy DLP Agents.

For example, if you want to install multiple agents on Windows 64-bit endpoints, you generate a single AgentInstaller_Win64.zip package. If you specify more than one installer for packaging, such as the Windows 64-bit agent installer and the Mac 64-bit agent installer, the system generates separate agent packages for each platform.

Note: Before you start generating the agent installation packages, confirm that the agent upgrader has been copied to the Enforce Server local file system. See “Downloading and extracting the upgrade software” on page 24.
Table 3-2 provides instructions for generating agent installation packages. The instructions assume you have deployed an Endpoint Server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Navigate to the <strong>Agent Packaging</strong> page.</td>
<td>Log on to the Enforce Server administration console as an administrator and navigate to the <strong>System &gt; Agents &gt; Agent Packaging</strong> page.</td>
</tr>
</tbody>
</table>
| 2    | Select one or more DLP Agent installation files.                       | Browse to the folder on the Enforce Server where you copied the agent installer files:  
- **Windows 64-bit**: AgentInstall64.msi  
- **Windows 32-bit**: AgentInstall.msi |
| 3    | Enter the server host name.                                            | Typically you enter the common name (CN) of the Endpoint Server host, or you can enter the IP address of the server.  
Be consistent with the type of identifier you use (CN or IP). If you used the CN for the Endpoint Server when deploying it, use the same CN for the agent package. If you used an IP address to identify the Endpoint Server, use the same IP address for the agent package.  
Alternatively, you can enter the CN or IP address of a load balancer server. |
| 4    | Enter the port number for the server.                                  | The default port is 10443. Typically you do not need to change the default port unless it is already in use or intended for use by another process on the server host. |
| 5    | Add additional servers (optional).                                     | Click the plus sign icon to add additional servers for failover.  
**Note:** Symantec Data Loss Prevention allots 2048 characters for Endpoint Server names. This allotment includes characters that are used for the Endpoint Server name, port numbers, and semicolons to delimit each server.  
The first server listed is primary; additional servers are secondary and provide backup if the primary is down. |
<p>| 6    | Enter the Endpoint tools password.                                     | A password is required to use the Endpoint tools to administer DLP Agents. The Endpoint tools password is case-sensitive. The password is encrypted and stored in a file on the Enforce Server. If you have to change this password, you must regenerate the agent package and redeploy the agents. You should store this password in a secure format of your own so that it can be retrieved if forgotten. |
| 7    | Re-enter the Endpoint tools password.                                  | The system validates that the passwords match and displays a message if they do not.                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Enter the target directory for the agent installation (Windows only).</td>
<td>The default installation directory for Windows 32- and 64-bit agents is %PROGRAMFILES%\Manufacturer\Endpoint Agent. Change the default path if you want to install the Windows agent to a different location on the endpoint host. You can only install the DLP Agent to an ASCII directory. <strong>Note:</strong> Include the drive letter if you plan to change the default directory. For example, use C:\Endpoint Agent. Not including a drive letter causes the agent installation to fail.</td>
</tr>
<tr>
<td>9</td>
<td>Enter the uninstall password key (optional, Windows only).</td>
<td>The use of an agent uninstall password is supported for Windows 32- and 64-bit agents. The uninstall password is a tamper-proof mechanism that requires a password to uninstall the DLP Agent.</td>
</tr>
<tr>
<td>10</td>
<td>Click <strong>Generate Installer Packages</strong>.</td>
<td>This action generates the agent installer package for each platform that you selected in step 3. If you are generating more than one package the generation process may take a few minutes.</td>
</tr>
<tr>
<td>11</td>
<td>Save the agent package ZIP file.</td>
<td>When the agent packaging process is complete, the system prompts you to download the agent installation package. Save the ZIP file to the local file system. Once you have done this you can navigate away from the <strong>Agent Packaging</strong> screen to complete the process. If you generated a single agent package, the ZIP file is named one of the following corresponding to the agent installer you uploaded: AgentInstaller_Win64.zip AgentInstaller_Win32.zip If you upload more than one agent installer, the package name is AgentInstallers.zip. The ZIP file contains separate ZIP files named as above containing the agent package for each platform you selected in step 3. See “Agent installation package contents” on page 38.</td>
</tr>
<tr>
<td>12</td>
<td>Install DLP Agents using the agent package.</td>
<td>Once you have generated and downloaded the agent package, you use it to install all agents for that platform.</td>
</tr>
</tbody>
</table>

**Agent installation package contents**

You generate the agent installation package for Windows and Mac agents at the **System > Agents > Agent Packaging** screen.
Note: When you upgrade agents, you generate the agent installation package and use the installation files to perform the agent upgrade.

See “Generating agent installation packages” on page 36.

The agent installation package for Windows agents contains the endpoint certificates, installation files, and the package manifest.

Table 3-3  
AgentInstaller_Win32.zip and AgentInstaller_Win64.zip installation package contents

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentInstall.msi or AgentInstall64.msi</td>
<td>Windows agent installer</td>
</tr>
<tr>
<td>endpoint_cert.pem</td>
<td>Agent certificate and encryption keys</td>
</tr>
<tr>
<td>endpoint_priv.pem</td>
<td>See “Working with endpoint certificates” on page 40.</td>
</tr>
<tr>
<td>endpoint_truststore.pem</td>
<td></td>
</tr>
<tr>
<td>install_agent.bat</td>
<td>Use to install the agent silently</td>
</tr>
<tr>
<td>upgrade_agent.bat</td>
<td>Use to upgrade the agent</td>
</tr>
<tr>
<td>PackageGenerationManifest.mf</td>
<td>Package metadata</td>
</tr>
</tbody>
</table>

The Mac agent package contains endpoint certificates, installation files, the package manifest, and a file to generate the installation script for the Mac OS.

Table 3-4  
AgentInstaller_Mac64.zip installation package contents

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentInstall.pkg</td>
<td>Mac agent installer</td>
</tr>
<tr>
<td>AgentInstall.plist</td>
<td>Mac agent installation properties configuration file</td>
</tr>
<tr>
<td>create_package</td>
<td>Use to generate the installation package for the Mac OS. You can use this package to install agents manually or using deployment tools like Apple Remote Desktop (ARD).</td>
</tr>
<tr>
<td>endpoint_cert.pem</td>
<td>Agent certificate and encryption keys</td>
</tr>
<tr>
<td>endpoint_priv.pem</td>
<td>See “Working with endpoint certificates” on page 40.</td>
</tr>
<tr>
<td>endpoint_truststore.pem</td>
<td></td>
</tr>
<tr>
<td>Install_Readme.rtf</td>
<td>Provides installation steps</td>
</tr>
</tbody>
</table>
Working with endpoint certificates

Symantec Data Loss Prevention automatically generates the SSL certificates and keys needed for authentication and secure communications between DLP Agents and Endpoint Servers.

See “About secure communications between DLP Agents and Endpoint Servers” on page 36.

When you install or upgrade the Enforce Server, the system generates the DLP root certificate authority (CA) certificate. This file is versioned and the version is incremented if the file is regenerated. You can view which CA version is currently in use at the System > Settings > General screen. The password for the DLP root CA is randomly generated and used by the system. Changing the root CA password is reserved for internal use.

When you deploy an Endpoint Server, the system generates the server public-private key pair signed by the DLP root CA certificate. These files are versioned. When you generate the agent package, the system generates the agent public-private key pair and the agent certificate, also signed by the DLP root CA.

See “Generating agent installation packages” on page 36.

The DLP root CA certificate and the server key pair are stored on the Enforce Server host file system in directory \SymantecDLP\protect\keystore (Windows) or /opt/SymantecDLP/protect/keystore (Linux). These files must remain in this directory for proper agent-server connectivity. If you remove or rename one or both of the server keys, the system regenerates them when you recycle the Endpoint Server. In this scenario you do not have to regenerate the agent certificates because the certificate authority is unchanged.

Do not rename or remove the DLP root CA certificate from the keystore directory. If you do you, you will need to regenerate the agent installation package and redeploy all agents because the DLP root CA is changed. To avoid this, you should back up the CA certificate and server keys, and secure them as you would other critical files.

Table 3-5 lists and describes the CA certificate and server keys generated by the system for secure agent-server communications.
Table 3-5  SSL certificates and keys for Endpoint Servers

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
<th>Generation</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate_authority_vX.jks</td>
<td>DLP root CA certificate</td>
<td>Initial: On install or upgrade of the Enforce Server.</td>
<td>Stored in the keystore directory on the Enforce Server host. Regeneration of the CA increments the version number in the file name, for example: certificate_authority_v2.jks certificate_authority_v3.jks If the CA is regenerated, you must regenerate the server and agent keys and redeploy the agents.</td>
</tr>
<tr>
<td>monitor###_truststore_vX.jks</td>
<td>Endpoint trust store for the agent to trust the server certificate (server public key)</td>
<td>Initial: On deployment of the Endpoint Server.</td>
<td>Stored in the keystore directory on the Enforce Server host. The number after “monitor” (###) is a server identifier. It is unique to each Endpoint Server. Regeneration of the server keystore and truststore increments the version number in the files, for example: monitor###_keystore_v2.jks monitor###_truststore_v2.jks If the server keys are regenerated, you do not have to regenerate the agent installation package.</td>
</tr>
<tr>
<td>monitor###_keystore_vX.jks</td>
<td>Server certificate, signed by the DLP root CA, and its private key</td>
<td>Initial: On deployment of the Endpoint Server.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-6 lists the SSL certificate and keys, and the passwords, generated during the agent installation packaging process.
### Table 3-6 SSL certificates and keys for DLP Agents

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
<th>Generation</th>
<th>Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint_cert.pem</td>
<td>Self-signed endpoint agent certificate</td>
<td>During the agent installation package process.</td>
<td>Deployed with the agent to each endpoint host.</td>
</tr>
<tr>
<td>endpoint_truststore.pem</td>
<td>Agent trust store for the server (root CA public key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>endpoint_priv.pem</td>
<td>Private key for the endpoint agent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Process to upgrade the DLP Agent on Windows

You can upgrade one DLP Agent to a Windows endpoint at a time, or you can use system management software (SMS) to upgrade many DLP Agents automatically. Symantec recommends that you upgrade one DLP Agent using the manual method before you upgrade many DLP Agents using your SMS. Upgrading in this manner helps you troubleshoot potential issues and ensure that upgrading using your SMS goes smoothly.

Before you upgrade DLP Agents on Windows endpoints, confirm that you have completed prerequisite steps. See “About Symantec Data Loss Prevention Agent upgrades” on page 34.

### Table 3-7 Process to upgrade agents on Windows endpoints

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prepare endpoints that have Safe Mode monitoring enabled.</td>
<td>See &quot;Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled&quot; on page 43.</td>
</tr>
</tbody>
</table>
Table 3-7  Process to upgrade agents on Windows endpoints (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2    | Upgrade the agent.  
Upgrade an agent manually.  
You can upgrade an agent manually when you want to test the configuration.  
Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time. | See “Upgrading the Windows agent manually” on page 43.  
See “Upgrading the Windows agent silently” on page 44. |

Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled

If you are upgrading DLP Agents from 12.5.x or 14.0.x with Safe Mode monitoring enabled to 14.5, you must delete the registry entries for the TDI drivers before you upgrade the agents.

Locate and delete the following TDI registry entries on each endpoint with Safe Mode monitoring enabled:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\tdifdvvvv.sys]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\tdifdvvvv.sys]

For the file tdifdvvvv.sys, replace vvvv with the DLP Agent version. For example, DLP Agent version 12.5.2 would display as tdifd1252.sys.

Upgrading the Windows agent manually

You can upgrade DLP Agents manually on your endpoints by using the upgrade_agent.bat file. Under normal circumstances, you upgrade DLP Agents manually when you troubleshoot or test DLP Agents in your implementation.

These steps assume that you have generated the agent installation package. See “Generating agent installation packages” on page 36.
To install the DLP Agent manually

1 Run the DLP Agent upgrade batch file.
   You run the `upgrade_agent.bat` located in the agent installation package ZIP file. The user running the batch file must have administrator rights.

2 Confirm that the agent is running.
   Once installed, the DLP Agent initiates a connection with the Endpoint Server. Confirm that the agent is running by going to **Agent > Overview** and locating the agent in the list.

Upgrading the Windows agent silently

You can upgrade DLP Agents silently using a systems management software (SMS) product. Symantec recommends that you use the `upgrade_agent.bat` package to upgrade agents. You must upgrade agents from a local directory. If you do not upgrade from a local directory, some functions of the DLP Agent are disabled.

---

**Note:** These steps assume that you have generated the agent installation package. See “Generating agent installation packages” on page 36.
To perform a silent upgrade

1. In your SMS package, specify the `upgrade_agent.bat` package.

**Note:** Do not rename the `upgrade_agent.bat` file for any reason. If you rename this file, your systems management software cannot recognize the file and the installation fails.
2 Specify the `upgrade_agent.bat` installation properties.

When you install the Symantec DLP Agent, your systems management software issues a command to the specified endpoints. The following is an example of what the command might look like:

```
msiexec /i InstallAgent.bat /q INSTALLDIR="C:\Program Files\Manufacturer\Symantec DLP Agent" ARPSYSTEMCOMPONENT="1" ENDPOINTSERVER="epserver:8001" SERVICENAME="ENDPOINT" WATCHDOGNAME="WATCHDOG" UNINSTALLPASSWORDKEY="password" TOOLS_KEY="<tools key password>" ENDPOINT_CERTIFICATE="endpoint_cert.pem" ENDPOINT_PRIVATEKEY="endpoint_priv.pem" ENDPOINT_TRUSTSTORE="endpoint_truststore.pem" ENDPOINT_PRIVATEKEY_PASSWORD="<endpoint private key password>" VERIFY_SERVER_HOSTNAME="No" STARTSERVICE="Yes" ENABLEWATCHDOG="YES" LOGDETAILS="Yes" /log C:\installAgent.log
```

The following table outlines each command and what it does.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msiexec</td>
<td>The Windows command for executing MSI packages.</td>
</tr>
<tr>
<td>/i</td>
<td>Specifies the name of the package.</td>
</tr>
<tr>
<td>/q</td>
<td>Specifies a silent install.</td>
</tr>
<tr>
<td>ARPSYSTEMCOMPONENT</td>
<td>Optional properties to msiexec.</td>
</tr>
<tr>
<td>ENDPOINTSERVER, SERVICENAME, INSTALLDIR, UNINSTALLPASSWORDKEY, and WATCHDOGNAME</td>
<td>Properties for the agent installation package.</td>
</tr>
<tr>
<td>TOOLS_KEY, ENDPOINT_CERTIFICATE, ENDPOINT_PRIVATEKEY, ENDPOINT_TRUSTSTORE, ENDPOINT_PRIVATEKEY_PASSWORD, and VERIFY_SERVER_HOSTNAME</td>
<td>Properties that reference the files and the passwords that are associated with the agent certificates.</td>
</tr>
</tbody>
</table>

3 Specify the `msiexec` properties.

For details on entering this information into your particular systems management software, see the software product documentation.
**Note:** You can find additional installation command examples in DLPDownloadHome\DLP\14.5\Endpoint\x64\install_agent64.bat or DLPDownloadHome\DLP\14.5\Endpoint\x86\install_agent.bat.

After you upgrade the agents, the DLP Agent service automatically starts on each endpoint computer. Log on to the Enforce Server and go to System > Agents > Overview, then locate the upgraded agent. Verify that the newly upgraded agent is registered (the services should appear in the list).

See “About Symantec Data Loss Prevention Agent upgrades” on page 34.

### Process to upgrade the DLP Agent on Mac

You can upgrade one DLP Agent to a Mac endpoint at a time, or you can use system management software (SMS) to upgrade many DLP Agents automatically. Symantec recommends that you upgrade one DLP Agent using the manual method before you upgrade many DLP Agents using your SMS. Upgrading in this manner helps you troubleshoot potential issues and ensure that upgrading using your SMS goes smoothly.

Before you upgrade DLP Agents on Mac endpoints, confirm that you have completed prerequisite steps. See “About Symantec Data Loss Prevention Agent upgrades” on page 34.

#### Table 3-8 Process to install agents on Mac endpoints

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Package the Mac agent installation files. You compile the Mac agent installation files into one PKG file. You later use this file to manually upgrade an agent, or to insert in your SMS to upgrade many Mac endpoint agents simultaneously. You can also add endpoint tools to the package and add a custom package identifier.</td>
<td>See “Packaging Mac agent upgrade files” on page 48.</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade the agent. Upgrade an agent manually. You can upgrade an agent manually when you want to test the configuration. Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time.</td>
<td>See “Upgrading the DLP Agent for Mac manually” on page 50. See “Upgrading DLP Agents on Mac endpoints silently” on page 51.</td>
</tr>
</tbody>
</table>
Table 3-8  Process to install agents on Mac endpoints (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Confirm that the Mac agent service is running.</td>
<td>See “Confirming that the Mac agent is running” on page 52.</td>
</tr>
<tr>
<td>4</td>
<td>(Optional) Review the upgraded Mac agent components.</td>
<td>See “What gets upgraded for DLP Agents on Mac endpoints” on page 52.</td>
</tr>
<tr>
<td></td>
<td>These components include the drivers that prevent tampering and keep</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the agent running.</td>
<td></td>
</tr>
</tbody>
</table>

Packaging Mac agent upgrade files

You use the create_package tool to bundle the Mac agent upgrade-related files into a single package. You place this package in your SMS software to perform a silent upgrade. You also use the create_package tool to assign a package ID and to bundle endpoint tools with the agent upgrade.

The following steps assume that you have generated the agent installation package and completed all prerequisites. See “About secure communications between DLP Agents and Endpoint Servers” on page 36.
To package the Mac agent upgrade files:

1. Locate the AgentInstaller_Mac64.zip agent installation package. Unzip the contents of this file to a folder on a Mac endpoint; for example use /tmp/MacInstaller.

   See “Agent installation package contents” on page 38.

2. Use the Terminal.app to bundle the Mac agent upgrade-related file by running the following commands:

   ```
   $ cd /tmp/MacInstaller
   Defines the path where the Mac agent upgrade files reside.
   
   $ ./create_package
   Calls the create_package tool.
   
   -i <com.company.xyz>
   (Optional) Includes a custom package identifier.
   
   You can register the DLP Agent installer receipt data with a custom package identifier. Replace <com.company.xyz> with information specific to your deployment.
   
   -t ./Tools
   (Optional) Calls the create_package tool to bundle the agent tools.
   
   See “About optional installation and maintenance tools” on page 50.
   ```

   The following is an example of what the completed command might look like:

   ```
   $ cd /tmp/MacInstaller; $ ./create_package; -i <com.company.xyz>; -t ./Tools
   ```

   After you execute the command, a message displays the package creation status.

   A file named AgentInstall_WithCertificates.pkg is created in the location you indicated. Based on the example above, AgentInstall_WithCertificates.pkg is created at /tmp/MacInstaller.

3. (Optional) If you opted to register the DLP Agent with a custom package identifier, execute the following command to verify the custom package identity:

   ```
   $ pkgutil --pkg-info <com.company.xyz>
   ```

   Replace com.company.xyz with information specific to your deployment.
About optional installation and maintenance tools

You can opt to include installation and maintenance tools with the Mac agent installation package. After the agent installs, administrators can run these tools on Mac endpoints.

The tools can be found in the following files:

- Installation tools are found in the `Symantec_DLP_14.5_Agent_Mac-IN.zip` file.
- Maintenance tools are found in the `SymantecDLPMacAgentTools_14.5.zip` file.

See the topic "About Endpoint tools" in the *Symantec Data Loss Prevention Administration Guide*.

Place tools you want to include in the PKG in the same directory where the PKG file is located; for example use `/tmp/MacInstaller`.

See “Packaging Mac agent upgrade files” on page 48.

Table 3-9 lists the available tools.

### Table 3-9: Mac agent installation and maintenance tools

<table>
<thead>
<tr>
<th>Tool type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Installation | ■ Agent.ver adds agent package versioning information.  
■ Start_agent restarts the Mac agents that have been shut down on the Agent List screen.  
■ Uninstall_agent uninstalls the DLP Agent from Mac endpoints. |
| Maintenance  | ■ Vontu_sqlite3 lets you inspect the agent database.  
■ Logdump creates agent log files. |

### Upgrading the DLP Agent for Mac manually

Table 3-10 provides steps for upgrading the DLP Agent for Mac manually.

Normally you perform a manual installation or upgrade when you want to test the agent installation package. If you do not plan to test the agent installation package, you install Mac agents using an SMS. See “Upgrading DLP Agents on Mac endpoints silently” on page 51.

**Note:** The following steps assume that you have generated the agent installation package and completed all prerequisites. See “About secure communications between DLP Agents and Endpoint Servers” on page 36.
### Table 3-10: Instructions for upgrading the DLP Agent on a Mac endpoint

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Locate the agent installation package ZIP (AgentInstaller_Mac64.zip), and unzip it to the Mac endpoint.</td>
<td>For example, unzip the file to /tmp/MacInstaller.</td>
</tr>
</tbody>
</table>
| 2    | Upgrade the Mac Agent from the command line using the Terminal application. | Run the following command on the target endpoint:  
```
$ sudo installer -pkg /tmp/AgentInstall/AgentInstall.pkg -target /
```
Replace /tmp/MacInstaller with the path where you unzipped the agent installation package. |
| 3    | Verify the Mac agent upgrade. | To verify the Mac agent installation, open the Activity Monitor and search for the edpa process. It should be up and running.  
The Activity Monitor displays processes being run by logged in user and edpa runs as root. Select View All Processes to view edpa if you are not logged in as root user.  
You can also confirm that agent was installed to the default directory: /Library/Manufacturer/Endpoint Agent. |
| 4    | (Optional) Troubleshoot the upgrade. | If you experience upgrade issues, use the Console application to check the log messages.  
Review the Mac Agent installer logs at /var/log/install.log.  
In addition, you can rerun the installer with -dumplog option to create detailed installation logs. For example, use the command sudo installer -pkg /tmp/AgentInstall/AgentInstall.pkg -target / -dumplog.  
Replace /tmp/MacInstaller with the path where you unzipped the agent installation package. |
| 5    | (Optional) Review information about the Mac agent installation. | See “What gets upgraded for DLP Agents on Mac endpoints” on page 52. |

**Upgrading DLP Agents on Mac endpoints silently**

You can use a silent upgrade process by using systems management software (SMS) to upgrade DLP Agents. You must always upgrade the agent installation package from a local directory. If you do not upgrade from a local directory, some functions of the DLP Agent are disabled.
These steps assume that you have generated the agent installation package and packaged the Mac agent installation files.

See “Generating agent installation packages” on page 36.

See “Packaging Mac agent upgrade files” on page 48.

To perform an unattended upgrade

1. Enable the SMS client on the Mac endpoints.
2. Obtain root user access to the Mac endpoints.
3. Specify the AgentInstall_WithCertificates.pkg package in your systems management software.
4. Specify a list or range of network addresses where you want to upgrade the DLP Agent.
5. Start the silent upgrade process.

Note: If messages indicate that the process failed, review the instal.log file that is located in the /tmp directory on each Mac endpoint.

Confirming that the Mac agent is running

To verify that the Mac agent is running, open the Console application and locate the launchd service. The launchd service is deployed during the agent installation and begins running after the installation completed.

Launchd is the service that automatically restarts the agent daemon if an endpoint user stops or kills the agent. Users cannot stop the launchd service on their workstations. Preventing users from stopping the launchd service allows the DLP Agent to remain active on the endpoint.

You can also confirm that the com.symantec.dlp.edpa service is running. This service displays pop-up notifications on the Mac endpoint.

See “What gets upgraded for DLP Agents on Mac endpoints” on page 52.

What gets upgraded for DLP Agents on Mac endpoints

When the DLP Agent is installed or upgraded on a Mac endpoint, a number of components are installed. Do not disable or modify any of these components or the DLP Agent may not function correctly.
## Table 3-11  Mac agent components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Endpoint Agent daemon (EDPA)** | The installation process places the EDPA files here: 
/Library/Manufacturer/Endpoint Agent.

The `com.symantec.manufacturer.agent.plist` file contains configuration settings for the Endpoint Agent daemon. This file is located at /Library/LaunchDaemons/. |
| **Encrypted database** | Each DLP Agent maintains an encrypted database at the endpoint. The database stores incident metadata in the database, contents on the host file system, and the original file that triggered the incident, if needed. The DLP Agent analyzes the content locally. |
| **Log files** | The DLP Agent logs information on completed and failed processes. |
| **Database (rrc.ead)** | This database maintains and contains non-matching entries for rules results caching (RRC). |
Post-upgrade tasks

This chapter includes the following topics:

- Performing post-upgrade tasks
- Restore additional JAR files
- Verifying Symantec Data Loss Prevention operations

Performing post-upgrade tasks

You must perform certain tasks after you finish upgrading.

See “Verifying Symantec Data Loss Prevention operations” on page 55.
See “Symantec Data Loss Prevention upgrade phases” on page 10.

Restore additional JAR files

The Symantec Data Loss Prevention upgrader does not replace any JAR files that you may have added to your deployment. For example, you might have added JDBC drivers for your Network Discover detection server for SQL database scans. You must manually restore these files after the upgrade process.
To restore additional JAR files after upgrade

1. Locate the backup location of your additional JAR files.
   For example, on Windows:
   C:\SymantecDLP_Backup\Files\Protect\lib\your_jar.jar
   On Linux:
   /opt/SymantecDLP_Backup\Files/Protect/lib/your_jar.jar

2. Copy the JAR files from your backup location to the same directory on your upgraded system.
   For example, on Windows:
   C:\SymantecDLP\Protect\lib\your_jar.jar
   On Linux
   /opt/SymantecDLP/Protect/lib/your_jar.jar

Verifying Symantec Data Loss Prevention operations

Verify that Symantec Data Loss Prevention operates correctly by performing some checks.

To verify Symantec Data Loss Prevention operations

1. Log on to the Enforce Server administration console as Administrator.

2. Log out of the Enforce Server administration console and then log on as a user other than Administrator.

3. Go to the System Overview screen and recycle the detection servers to verify that they are connected.

4. Click on each heading in the Enforce Server navigation pane to view the data that was carried over from the previous version.

5. Verify that any reports that you had saved from your previous version are still there.

6. Send test emails to trigger a few existing policies and then run a traffic report to confirm that the test messages generated incidents.

7. Network Discover provides incremental scanning for certain target types. After you upgrade Symantec Data Loss Prevention, verify that incremental scanning is configured for valid targets. See the Symantec Data Loss Prevention System Administration Guide for information about configuring incremental scans.
8 If you have deployed any Lookup plug-ins, go to the **System > Lookup Plugins** screen and verify that the plug-in appears in the list of plug-ins and is configured correctly.

9 Check the **Events** screen for any severe events.

For more information on performing these procedures, see the *Symantec Data Loss Prevention Administration Guide*.

See “Performing post-upgrade tasks” on page 54.
Starting and stopping Symantec Data Loss Prevention services

This chapter includes the following topics:

- About Symantec Data Loss Prevention services

About Symantec Data Loss Prevention services

The Symantec Data Loss Prevention services may need to be stopped and started periodically. This section provides a brief description of each service and how to start and stop the services on supported platforms.

The Symantec Data Loss Prevention services for the Enforce Server are described in the following table:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vontu Manager</td>
<td>Provides the centralized reporting and management services for Symantec Data Loss Prevention.</td>
</tr>
<tr>
<td>Vontu Monitor Controller</td>
<td>Controls the detection servers (monitors).</td>
</tr>
<tr>
<td>Vontu Notifier</td>
<td>Provides the database notifications.</td>
</tr>
<tr>
<td>Vontu Incident Persister</td>
<td>Writes the incidents to the database.</td>
</tr>
<tr>
<td>Vontu Update</td>
<td>Installs the Symantec Data Loss Prevention system updates.</td>
</tr>
</tbody>
</table>
Starting and stopping Symantec Data Loss Prevention services

About starting and stopping services on Windows

The procedures for starting and stopping services vary according to installation configurations and between Enforce and detection servers.

- See “Starting an Enforce Server on Windows” on page 58.
- See “Stopping an Enforce Server on Windows” on page 58.
- See “Starting a Detection Server on Windows” on page 59.
- See “Stopping a Detection Server on Windows” on page 59.
- See “Starting services on single-tier Windows installations” on page 60.
- See “Stopping services on single-tier Windows installations” on page 60.

Starting an Enforce Server on Windows

Use the following procedure to start the Symantec Data Loss Prevention services on a Windows Enforce Server.

To start the Symantec Data Loss Prevention services on a Windows Enforce Server

1. On the computer that hosts the Enforce Server, navigate to Start > All Programs > Administrative Tools > Services to open the Windows Services menu.

2. Start the Symantec Data Loss Prevention services in the following order:
   - Vontu Notifier
   - Vontu Manager
   - Vontu Incident Persister
   - Vontu Monitor Controller (if applicable)
   - Vontu Update (if necessary)

Note: Start the Vontu Notifier service first before starting other services.

Stopping an Enforce Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows Enforce Server.
To stop the Symantec Data Loss Prevention Services on a Windows Enforce Server

1. On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.

2. From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
   - Vontu Monitor Controller (if applicable)
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Notifier
   - Vontu Update (if necessary)

See “Starting an Enforce Server on Windows” on page 58.

Starting a Detection Server on Windows

To start the Symantec Data Loss Prevention services on a Windows detection server

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.

2. Start the Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Monitor
   - Vontu Update

See “Stopping a Detection Server on Windows” on page 59.

Stopping a Detection Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows detection server.

To stop the Symantec Data Loss Prevention Services on a Windows detection server

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.

2. From the **Services** menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Update
Starting services on single-tier Windows installations

Use the following procedure to start the Symantec Data Loss Prevention services on a single-tier installation on Windows.

To start the Symantec Data Loss Prevention services on a single-tier Windows installation

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.

2. Start the Symantec Data Loss Prevention in the following order:
   - Vontu Notifier
   - Vontu Manager
   - Vontu Incident Persister
   - Vontu Monitor Controller (if applicable)
   - Vontu Monitor
   - Vontu Update (if necessary)

   **Note:** Start the Vontu Notifier service before starting other services.

Stopping services on single-tier Windows installations

Use the following procedure to stop the Symantec Data Loss Prevention services on a single-tier installation on Windows.

To stop the Symantec Data Loss Prevention services on a single-tier Windows installation

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.

2. From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
   - Vontu Monitor

See “Starting a Detection Server on Windows” on page 59.

See “Stopping services on single-tier Windows installations” on page 60.
Starting and stopping Symantec Data Loss Prevention services

About Symantec Data Loss Prevention services

- Vontu Monitor Controller (if applicable)
- Vontu Incident Persister
- Vontu Manager
- Vontu Notifier
- Vontu Update (if necessary)

See “Starting services on single-tier Windows installations” on page 60.
Symantec Data Loss Prevention upgrade troubleshooting and recovery

This chapter includes the following topics:

- About troubleshooting Symantec Data Loss Prevention upgrade problems
- Troubleshooting Upgrade Wizard launch problems
- Correcting JAR file upload problems
- Manually uploading the JAR file to the Enforce Server
- Manually starting the Upgrade Wizard
- Reverting to the previous Symantec Data Loss Prevention release

About troubleshooting Symantec Data Loss Prevention upgrade problems

If you experience problems either with launching the Upgrade Wizard or with completing a successful product upgrade, see these topics:

- See “Troubleshooting Upgrade Wizard launch problems” on page 63.
- See “Reverting to the previous Symantec Data Loss Prevention release” on page 64.
Troubleshooting Upgrade Wizard launch problems

Occasionally, after trying to launch the Upgrade Wizard on the Enforce Server, you may observe a timeout or other error. This error can occur for several reasons:

- The upgrade JAR file failed to upload properly.
  See “Correcting JAR file upload problems” on page 63.
- If you receive the following error message, FIPS encryption is most likely enabled for your installation:
  "Unable to send redirect. System update did not succeed"
  This means that your browser cannot redirect from the Enforce Server Administration Console to the Upgrade Wizard user interface. In this case, you must manually browse to https://Enforce_server:8300.

Correcting JAR file upload problems

Occasionally, the upgrade JAR file fails to load correctly. This failure may result in a timeout of the Upgrade Wizard launch or another error.

Use one of the following methods to address JAR file upload errors:

- Browse to the Upgrade Wizard URL:
  https://Enforce_server:8300
  Where Enforce_server is the name of your Enforce Server. If you have changed the default port from 8300, use your new port instead.

- Click Upgrade again and repeat the upload of the upgrade JAR file.

If neither method works, then you must manually upload the JAR file to the Enforce Server.

See “Manually uploading the JAR file to the Enforce Server” on page 63.

Manually uploading the JAR file to the Enforce Server

If you encounter an error, such as a timeout, when uploading the upgrade JAR file to your Enforce Server, then upload the JAR file manually.

To manually upload the JAR file to the Enforce Server

1. Copy the upgrade JAR file 14.5_Upgrader_Windows.jar to the \SymantecDLP\Protect\updates directory.

2. Open Windows Explorer and go to the \SymantecDLP\Protect\updates directory.
Create a new directory that is named `enforceupgradeSymantecDLP` inside the `\SymantecDLP\Protect\updates` directory.

**Note:** The name of this directory must not contain any spaces.

Extract the contents of the upgrade JAR file `14.5_Upgrader_Windows.jar` into the `enforceupgradeSymantecDLP` directory. You can use Winzip or WinRAR to extract the contents of the JAR file.

You may now manually start the Upgrade Wizard.

See “Manually starting the Upgrade Wizard” on page 64.

---

**Manually starting the Upgrade Wizard**

Follow this procedure if you must manually start the Upgrade Wizard.

**To manually start the Upgrade Wizard**

1. Run `start_upgrade_wizard.bat`, which is located in the `\SymantecDLP\Protect\updates\enforceupgradeSymantecDLP` directory.
2. Wait a few minutes for the Upgrade Wizard server to start.
3. Open a Web browser and go to: `https://Enforce_server:8300`
   
   where `Enforce_server` is the name or IP address of your Enforce Server. If you have changed the default port from 8300, then you use your new port instead.
   
   The Web browser displays the Upgrade Wizard logon page.
4. Continue using the standard upgrade procedures.
   
   See “Performing an upgrade with the Upgrade Wizard” on page 27.

---

**Reverting to the previous Symantec Data Loss Prevention release**

If you experience problems with the new version of Symantec Data Loss Prevention, you can revert to the previous release.

To restore a previous release, you must have the following available:

- The Symantec Data Loss Prevention uninstaller and installer utilities. During installation of Symantec Data Loss Prevention, the uninstaller is saved on the host file system in the `\SymantecDLP` directory.
- The Symantec Data Loss Prevention license file for your deployment.
If your deployment uses Symantec Management Console, the host name or IP address of the Symantec Management Console server to use for managing Symantec Data Loss Prevention Endpoint Agents.

- A backup of the Symantec Data Loss Prevention Oracle database. For more information, see the *Symantec Data Loss Prevention System Maintenance Guide*.

- The location of the Oracle Base and Home directories.

- The Administrator credentials for your Symantec Data Loss Prevention deployment.

- The credentials for connecting to the Oracle database.

- The type of authentication that is used in your Symantec Data Loss Prevention deployment.

- The host name or IP address and port number that the Enforce Server uses to communicate with the Oracle database.

- A backup copy of the \SymantecDLP\Protect\config directory. The Upgrade Wizard automatically backs up this directory.

  When Symantec Data Loss Prevention is upgraded to a newer release, the upgrade process first saves the existing installation in a backup file. The backup file is created as a compressed file that resides under \SymantecDLP\Protect\updates\SymantecDLPServerBackup\, where *Server* specifies an Enforce or detection server.

- The EnforceReinstallationResources.zip file for your Enforce Server. See “Creating the Enforce Reinstallation Resources file” on page 65.

  See “Reverting the Enforce Server to a previous release” on page 66.

  See “Reverting a detection server to the previous release” on page 68.

### Creating the Enforce Reinstallation Resources file

If you have not previously uninstalled Symantec Data Loss Prevention, you must create an EnforceReinstallationResources.zip file from the \
SymantecDLP\Protect\updates\SymantecDLPEnforceBackup\SymantecDLPEnforceBackup_previousVersion.zip file. This file includes the CryptoMasterKey.properties file and the keystore files for your previous Symantec Data Loss Prevention deployment.

Follow this procedure to create the EnforceReinstallationResources.zip file required by the Symantec Data Loss Prevention 14.5 installer.
To create the Enforce Reinstallation Resources file

1. Extract the contents of the\SymantecDLP\Protect\updates\SymantecDLPEnforceBackup\SymantecDLPEnforceBackup_previousVersion.zip file to a temporary directory (line breaks added for legibility).

2. Copy the CryptoMasterKey.properties from \temp\SymantecDLP\Protect\updates\SymantecDLPEnforceBackup\config to a new folder named config.

3. Copy all the contents of the \temp\SymantecDLP\Protect\keystore folder to a new folder named keystore.

4. Create a ZIP archive that includes the config and keystore files. Name the new ZIP archive EnforceReinstallationResources.zip.

5. Use this new EnforceReinstallationResources.zip when reinstalling Symantec Data Loss Prevention from your backup version.

Reverting the Enforce Server to a previous release

If the upgrade procedure fails for any reason, you can restore the previous versions of Symantec Data Loss Prevention. The procedure that is described in this section applies to any type of Symantec Data Loss Prevention installation (single-tier, two-tier, and three-tier).

To revert an Enforce Server upgrade to the previous release

1. Stop all Symantec Data Loss Prevention services that are running on the Enforce Server.

   See “About Symantec Data Loss Prevention services” on page 57.

2. Stop all the Oracle services.

3. Restore the Symantec Data Loss Prevention Oracle database from the latest backup.

   Consult your Oracle documentation for more information.

4. Restart all the Oracle services.

   Consult your Oracle documentation for more information.
5 Copy the backup ZIP file that was created by the Upgrade Wizard to a location outside of the DLP installation. The file is located in the following directory:
\SymantecDLP\Protect\updates\SymantecDLPEnforceBackup\.

Open the directory with the most recent timestamp. Inside this directory there is a ZIP file named SymantecDLPEnforceBackup_previousVersion.zip that contains the backed-up files.

6 Launch the uninstall utility.

Navigate to Start > Symantec Data Loss Prevention > Symantec Data Loss Prevention Uninstaller.

Note: If the uninstaller executable fails or is not available on the Enforce Server host, you must manually uninstall the software. See “Manually uninstalling the Enforce Server or a detection server” on page 69.

7 Deselect Preserve Reinstallation Resources to indicate that the uninstaller should not create a new EnforceReinstallationResources.zip. Use the EnforceReinstallationResources.zip you created from the files in your backup directory.

See “Creating the Enforce Reinstallation Resources file” on page 65.

8 Click Next.

When the uninstall process is finished the Uninstall Complete panel appears.

9 Click Done.

10 Reinstall Symantec Data Loss Prevention.

Follow the instructions for installing the Enforce Server in the Symantec Data Loss Prevention Installation Guide for the version of Symantec Data Loss Prevention you are reinstalling.

Note the following before reinstalling Symantec Data Loss Prevention:

- Use the installer executable for the version of Symantec Data Loss Prevention that was deployed before you attempted the upgrade. You can only revert to this version of Symantec Data Loss Prevention. You may need to extract the Symantec Data Loss Prevention software ZIP file to locate the installer executable.

- When you run the installer, you are prompted for the type of server you are installing. Select either Enforce or Detection, or select the Single Tier option to install both the Enforce and Detection servers on a single computer.
When you reinstall the Enforce Server, deselect the option to **Initialize the Database**.

11. Stop all Symantec Data Loss Prevention services on the Enforce Server host.

12. Delete the following directory:

```bash
\SymantecDLP\Protect\config
```

13. Locate the backup ZIP file that you saved in step 5 and extract it to a temporary directory.

14. Copy the backup copy of the `Protect\config` directory from the temporary directory that you created in step 13 to the `\SymantecDLP\Protect\config` directory.

15. Restart the Symantec Data Loss Prevention services.

### Reverting a detection server to the previous release

If the upgrade of a detection server fails you can manually upgrade the detection server.

See “Reverting to the previous Symantec Data Loss Prevention release” on page 64.

To revert a detection server upgrade to the previous release:

1. Stop all Symantec Data Loss Prevention services that are running on the detection server host.

2. Copy the backup ZIP file created by the Upgrade Wizard to a location outside of the DLP installation. The file is located in the following directory:

```bash
\SymantecDLP\Protect\updates\SymantecDLPDetectionBackup\.
```

Open the directory with the most recent timestamp. Inside this directory there is a ZIP file named `SymantecDLPDetectionBackup_previousVersion.zip` that contains the backed-up files.

3. Uninstall the detection server software.

Double-click the following file on the detection server host:

```bash
\SymantecDLP\uninstall.exe
```

---

**Note:** If the uninstaller executable is not available on the detection server host, you may need to extract the Symantec Data Loss Prevention software ZIP file to locate the uninstaller executable.

If the uninstaller fails, you can manually uninstall the detection server. See “Manually uninstalling the Enforce Server or a detection server” on page 69.
4 Delete the following directory and its contents:
\SymantecDLP

5 Reinstall the detection server. You must use the correct version of the installer for the version to which you are upgrading.

Follow the instructions for installing a detection server in the *Symantec Data Loss Prevention Installation Guide for Windows* for the version of Symantec Data Loss Prevention that your are installing.

Note the following before reinstalling Symantec Data Loss Prevention:

- Use the installer executable for the version of Symantec Data Loss Prevention that was deployed before you attempted the upgrade. You can only revert to this version of Symantec Data Loss Prevention. You may need to extract the Symantec Data Loss Prevention software ZIP file to locate the installer executable.
- When you run the installer, you are prompted for the type of server you are installing. Select Detection.

6 If you have made any manual changes to configuration files on the file system of the detection server host, you must restore those configuration files from the backup created by the Upgrade Wizard.

Locate the backup ZIP file that you saved in step 2 and extract the file using WinRAR to a temporary directory. The detection server configuration files are located in the following directory: \SymantecDLP\Protect\config

7 Restart the Symantec Data Loss Prevention services.

**Manually uninstalling the Enforce Server or a detection server**

If the uninstall utility fails, you can use the following steps to uninstall an Enforce Server or a detection server.

**To manually uninstall Symantec Data Loss Prevention servers**

1 Stop all Symantec Data Loss Prevention processes.

2 Delete the following directory and its contents:
\SymantecDLP

3 Remove each service by running the following command:

```
sc delete <service name>
```

Where `<service name>` is the name of the service.

4 Use the **Local Users and Groups** tab in the Computer Management administration tool to delete the Symantec Data Loss Prevention user.
Agent configuration
  updating 32
Agent upgrade 14, 23, 34, 43–44

Backward compatibility
  Symantec DLP Agents and servers 14

Detection servers
  14_5DetectionUpgradePackage.jar file 32
  local upgrade 30–31
  requirements 14
  reverting to the previous release 68
  start_local_upgrade.bat file 32
  Upgrade Wizard 25

disk space 14
DLPDownloadHome directory 24

Endpoint Prevent group directories
  upgrading 33
Enforce Server
  requirements 14
  errors 63

FIPS encryption
  Upgrade Wizard 63

F
language packs
  upgrading 17
languages
  language packs 17
Linux operating system 14
  local upgrade 31
  14_5DetectionUpgradePackage.jar file 32
  start_local_upgrade.bat file 32
  upgrade directory 32

mixed operating systems 14

operating systems, mixed 14
Oracle database
  preparations 12

post-upgrade tasks 54
  restore additional JAR files 54
  verifying 55
preparations
  detection servers 25
  Oracle database 12
  scans, halting 20
  software download 24

requirements
  Enforce Server 14
reverting upgrade
  detection servers 68

scanners 33
scans, halt before upgrading 20
Skip Remaining Servers option 30

known issues 17
software download 24

start_local_upgrade.bat file 32

Symantec DLP Agent
  backward compatibility for agents and servers 14
  installing with system management software 51
  Mac
    installed aspects 52
    upgrade 47
  upgrading major versions manually 43
  upgrading major versions silently 44
  upgrading versions 34

Unable to send redirect message 63

upgrade 54
  See also post-upgrade tasks
  detection servers 25
  disk space 14
  errors, upload 63
  JAR file, manual upload 63
  known issues 17
  operating systems, mixed 14
  Oracle database 12
  phases 10
  requirements 14
  scanners 33
  scans, halting 20
  software download 24
  stages 10
  verifying 55

upgrade directory 32

Upgrade Wizard
  detection servers 25
  FIPS encryption 63
  JAR file, manual upload 63
  Skip Remaining Servers option 30
  starting 26
  starting, manually 64
  upload errors 63

upgrading
  major versions 34

V

verifying the upgrade 55

Vontu services
  starting 58–60
  stopping 58–60

Windows operating system 14