Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, CloudSOC, Blue Coat, the Symantec Logo, the Checkmark Logo, the Blue Coat logo, and the Shield 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.
Installing the Java Runtime Environment for a single-tier installation .......................................................... 37
Installing a single-tier server .................................................................................................................. 38
Running the Migration Utility on single-tier installation ..................................................................... 38
Verifying that the Enforce Server and the detection servers are running .............................................. 41
Applying the updated configuration to Endpoint Prevent servers ......................................................... 42
Upgrading your scanners ......................................................................................................................... 43
Upgrading Endpoint Prevent group directory connections .................................................................. 43

Chapter 3  Upgrading Symantec DLP Agents .......................................................... 44
About Symantec Data Loss Prevention Agent upgrades .............................................................. 44
About secure communications between DLP Agents and Endpoint Servers ........................................ 45
Process to upgrade the DLP Agent on Windows .............................................................................. 52
Process to upgrade the DLP Agent on Mac .................................................................................... 56

Chapter 4  Post-upgrade tasks ....................................................................................... 63
Performing post-upgrade tasks ........................................................................................................... 63
Verifying Symantec Data Loss Prevention operations ................................................................... 63
Migrating plug-ins ............................................................................................................................... 64
About securing communications between the Enforce Server and the database ................................ 65
About orapki command line options ............................................................................................... 65
Using orapki to generate the server certificate on the Oracle database ........................................... 66
Configuring communication on the Enforce Server ..................................................................... 68
Configuring the server certificate on the Enforce Server ........................................................... 70
Verifying the Enforce Server-database certificate usage .................................................................. 71

Chapter 5  Starting and stopping Symantec Data Loss Prevention services ................................... 73
About Symantec Data Loss Prevention services ........................................................................... 73
Starting and stopping services on Linux ......................................................................................... 75

Chapter 6  Symantec Data Loss Prevention upgrade troubleshooting and recovery ................................ 78
About troubleshooting Symantec Data Loss Prevention upgrade problems ...................................... 78
Troubleshooting Enforce Server services ......................................................................................... 79
Rolling back to the previous Symantec Data Loss Prevention release ................................................................................. 79
Reverting the Enforce Server to a previous release ....................... 80
Reverting a detection server to the previous release ................. 80
Creating the Enforce Reinstallation Resources file .................... 81
Uninstalling a server from a Linux system ............................... 82

Index .................................................................................................................... 84
Preparing to upgrade
Symantec Data Loss Prevention

This chapter includes the following topics:

- About updates to the Symantec Data Loss Prevention Upgrade Guide
- 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
- Supported upgrade backward compatibility for agents and servers
- About the requirement for language pack upgrades
- Upgrade requirements and restrictions
- Preparing your system for the upgrade
- About external storage for incident attachments

About updates to the Symantec Data Loss Prevention Upgrade Guide

This guide is occasionally updated as new information becomes available. You can find the latest version of the Symantec Data Loss Prevention Upgrade Guide at the following link to the Symantec Support Center article: http://www.symantec.com/docs/DOC9258.
Subscribe to the article at the Support Center to be notified when there are updates.

The following table provides the history of updates to this version of the Symantec Data Loss Prevention Upgrade Guide.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 October 2018</td>
<td>Corrected the path to service configuration files.</td>
</tr>
<tr>
<td></td>
<td>Added the location where you unzip the Update Readiness tool.</td>
</tr>
</tbody>
</table>

### About preparing to upgrade Symantec Data Loss Prevention

To review the new features for Symantec Data Loss Prevention 15.1, see the *What’s New and What’s Changed in Symantec Data Loss Prevention 15.1*: [http://www.symantec.com/docs/DOC10601](http://www.symantec.com/docs/DOC10601)

You can upgrade from Symantec Data Loss Prevention version 14.x or later to the latest version. From Symantec Data Loss Prevention 12.x you can upgrade to version 14.x, then to the latest version.

Symantec Data Loss Prevention 15.1 enables you to upgrade version 14.x detection servers in stages, while still using non-upgraded detection servers to monitor and prevent confidential data loss. To upgrade to version 15.1, you begin by upgrading the Enforce Server. The upgraded Enforce Server can communicate with version 14.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.

**Note:** If you are running DLP Agents on version 12.5.x, upgrade them to 14.x before you upgrade detection servers to the latest Symantec Data Loss Prevention version. Version 12.5.x agents cannot communicate with version 15.1 detection servers.

See “Supported upgrade backward compatibility for agents and servers” on page 17.

See “Upgrade requirements and restrictions” on page 21.

Back up your database before any upgrade. See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* for more information.
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>Review important information about the new release before starting the upgrade, including:</td>
<td>See the Symantec Data Loss Prevention 15.1 Release Notes at <a href="http://www.symantec.com/docs/DOC10600">http://www.symantec.com/docs/DOC10600</a> to learn about any known upgrade issues or issues with the current release of Symantec Data Loss Prevention. See What's New and What's Changed at <a href="http://www.symantec.com/docs/DOC10601">http://www.symantec.com/docs/DOC10601</a> for information about new and changed features in Symantec Data Loss Prevention 15.1. See “About the minimum system requirements for upgrading to the current release” on page 16. See “About the requirement for language pack upgrades” on page 21.</td>
</tr>
<tr>
<td></td>
<td>■ Known release issues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Minimum system requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Language pack requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ What's New and What's Changed.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Prepare the system for upgrading. This preparation includes the following items:</td>
<td>See “Preparing your system for the upgrade” on page 22.</td>
</tr>
<tr>
<td></td>
<td>■ Back up the Oracle database and detection server data. If the upgrade fails you can use these backups to restore your system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Prepare and run the Update Readiness tool. If you find issues, fix them before you upgrade to version 15.1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Create the Enforce Reinstallation Resources file. If the upgrade fails you can use these backups to restore your system.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Download and extract the version 15.1 software.</td>
<td>See “Downloading and extracting the upgrade software” on page 26.</td>
</tr>
</tbody>
</table>
Table 1-2  Symantec Data Loss Prevention upgrade phases (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4     | Upgrade the Enforce Server, which includes the following steps:  
■ Install the Java Runtime Environment.  
■ Install the version 15.1 Enforce Server.  
■ Migrate the previous version to the version 15.1 Enforce Server. | See “Migrating previous version data to a new Enforce Server installation” on page 27.  
See “Migrating previous version data to a new single-tier installation” on page 37. |
| 5     | Upgrade detection servers, which includes the following steps:  
■ Install the Java Runtime Environment.  
■ Install the version 15.1 detection server.  
■ Migrate the previous version to the version 15.1 detection server. | See “Migrating a previous version detection server to the latest version” on page 32. |
| 6     | Upgrade Symantec Data Loss Prevention Agents.  
**Note:** If you are running DLP Agents on version 12.5.x, upgrade them to 14.x before you upgrade detection servers to the latest Symantec Data Loss Prevention version. Version 12.5.x agents cannot communicate with version 15.1 detection servers.  
See “Supported upgrade backward compatibility for agents and servers” on page 17. | See “About Symantec Data Loss Prevention Agent upgrades” on page 44. |
| 7     | Upgrade any scanners. | See “Upgrading your scanners” on page 43. |
| 8     | Complete the required and optional post-upgrade tasks. | See “Performing post-upgrade tasks” on page 63. |

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 15.1:

■ Run the Update Readiness tool to confirm that the Oracle database is ready to upgrade to Symantec Data Loss Prevention version 15.1.  
See “Checking the database update readiness” on page 11.
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 following guide available at the Symantec Support Center:

- Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide:
  http://www.symantec.com/docs/DOC10713

Make note of the location of the Oracle home directory on your Enforce Server (this directory is needed later). The home directory is the directory for the installation of the Oracle client tools. This directory functions as the local client installation directory when Enforce uses a remote database. The remote database can be running on Linux, Windows, or any other operating system that the Oracle database can run on. If you installed Oracle 11g using the default options, then the Oracle home is /opt/oracle/product/11.2.0.4/db_1.

On single- and two-tier installations, add SQL*Plus to the Protect user's path to fetch database diagnostics information for the Tablespace Summary page.

To add SQL*Plus to the Protect user path

1. On the Enforce Server host computer, log on as the protect user.

   su protect

2. Open the .bash_profile file in a text editor.

3. Add the SQL*Plus directory to the path:

   export ORACLE_HOME=/opt/oracle/product/11.2.0.4/db_1
   export PATH=$ORACLE_HOME/bin: $PATH

4. Save and close the .bash_profile file.

5. Restart the Enforce Server host computer to apply your changes.

See “Preparing your system for the upgrade” on page 22.

Checking the database update readiness

You use the Update Readiness tool to confirm that the Oracle database is ready to upgrade to the next Symantec Data Loss Prevention version.

The Update Readiness tool tests the following items in the database schema:

- Oracle version
- Oracle patches
- Permissions
- Tablespaces
- Existing schema against standard schema
- Real Application Clusters
- Change Data Capture
- Virtual columns
- Partitioned tables
- Numeric overflow
- Temp Oracle space

Table 1-3 lists tasks you complete to run the tool.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Locate the latest version of the tool.</td>
<td>See “Preparing the Update Readiness tool” on page 12.</td>
</tr>
<tr>
<td>2</td>
<td>Create the Update Readiness tool database account.</td>
<td>See “Creating the Update Readiness tool database account” on page 13.</td>
</tr>
<tr>
<td>3</td>
<td>Run the tool.</td>
<td>See “Running the Update Readiness tool for Symantec Data Loss Prevention version 14.x and 15.0” on page 14.</td>
</tr>
<tr>
<td>4</td>
<td>Review the update readiness results.</td>
<td>See “Reviewing update readiness results” on page 16.</td>
</tr>
</tbody>
</table>

Preparing the Update Readiness tool

Preparing the Update Readiness tool includes downloading the tool and moving it to the Enforce Server.
To prepare the Update Readiness tool

1. Obtain the latest version of the tool (for both major or minor release versions of Symantec Data Loss Prevention) from Software Downloads.

   The tool file name is `Symantec_DLP_15.1_Update_Readiness_Tool_15.1.0-1.zip`. The tool version changes when updated tools are released.

   The latest version of the Update Readiness tool includes important fixes and improvements, and should be the version that you use before attempting an upgrade. See the Support Center article About the Symantec Data Loss Prevention Update Readiness tool, and URT test results for information about the latest version; subscribe to the article to be informed about new versions.

   Symantec recommends that you download the tool to the `DLP\DLP\15.1\` directory.

   **Note:** Review the Readme file that is included with the tool for a list of Symantec Data Loss Prevention versions the tool is capable of testing.

2. Unzip the tool.

   - **Windows:** `c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\Migrator\`
   - **Linux:** `opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/Migrator/`

   During the upgrade process, the Migration Utility checks the database update readiness by running the Update Readiness tool from this location.

   See "Checking the database update readiness" on page 11.

### Creating the Update Readiness tool database account

Before you can run the Update Readiness tool, you must create a database account.

**To create the new Update Readiness tool database account**

1. Navigate to the `/script` folder where you extracted the Update Readiness tool.

2. Start SQL*Plus:

   ```bash
   sqlplus /nolog
   ```

3. Run the `oracle_create_user.sql` script:

   ```sql
   SQL> @oracle_create_user.sql
   ```
4 At the Please enter the password for sys user prompt, enter the password for the SYS user.

5 At the Please enter sid prompt, enter a user name.

6 At the Please enter required username to be created prompt, enter a name for the new upgrade readiness database account.

7 At the Please enter a password for the new username prompt, enter a password for the new upgrade readiness database account.

   Use the following guidelines to create an acceptable password:

   ■ Passwords cannot contain more than 30 characters.
   ■ Passwords cannot contain double quotation marks, commas, or backslashes.
   ■ Avoid using the & character.
   ■ Passwords are case-sensitive by default. You can change the case sensitivity through an Oracle configuration setting.
   ■ If your password uses special characters other than _, #, or $, or if your password begins with a number, you must enclose the password in double quotes when you configure it.

   Store the user name and password in a secure location for future use. You use this user name and password to run the Update Readiness tool.

8 As the database sysdba user, grant permission to the Symantec Data Loss Prevention schema user name for the following database objects:

   sqlplus sys/[schema user name] as sysdba
   GRANT READ,WRITE ON directory DATA_PUMP_DIR TO [schema user name];
   GRANT SELECT ON dba_registry_history TO [schema user name];
   GRANT SELECT ON dba_temp_free_space TO [schema user name];

   See “Preparing the Update Readiness tool” on page 12.
   See “Checking the database update readiness” on page 11.

Running the Update Readiness tool for Symantec Data Loss Prevention version 14.x and 15.0

After you locate the update readiness tool, you run it from the command prompt on the server where the Enforce Server is installed. This procedure applies to Symantec Data Loss Prevention 14.x, 15.0, and 15.0 MP1.
To run the Update Readiness tool

1. From a command window, go to the directory where you extracted the Update Readiness tool:
   
   c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\Migrator\ for Windows computers
   
   opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/Migrator/ for Linux computers

2. Run the Update Readiness tool using the following command:

   ```java
   java UpdateReadinessTool
   --username <schema user name>
   --password <password>
   --readiness_username <readiness_username>
   --readiness_password <readiness_password>
   --sid <database_system_id>
   [--quick]
   ```

The following table identifies the commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;schema user name&gt;</td>
<td>The Symantec Data Loss Prevention schema user name.</td>
</tr>
<tr>
<td>&lt;password&gt;</td>
<td>The Symantec Data Loss Prevention schema password.</td>
</tr>
<tr>
<td>&lt;readiness_username&gt;</td>
<td>The Update Readiness tool database account user you created.</td>
</tr>
<tr>
<td></td>
<td>See &quot;Creating the Update Readiness tool database account&quot; on page 13.</td>
</tr>
<tr>
<td>&lt;readiness_password&gt;</td>
<td>The password for the Update Readiness tool database account user.</td>
</tr>
<tr>
<td>&lt;database_system_id&gt;</td>
<td>The database system ID (SID), typically &quot;protect.&quot;</td>
</tr>
<tr>
<td>[--quick]</td>
<td>The optional command only runs the database object check and skips the update readiness test.</td>
</tr>
</tbody>
</table>

After the test completes, you can locate the results in a log file in the /output directory. This directory is located where you extracted the Update Readiness tool. If you do not include [--quick] when you run the tool, the test may take up to an hour to complete. You can verify the status of the test by reviewing log files in the /output directory.

See "Preparing the Update Readiness tool" on page 12.

See "Reviewing update readiness results" on page 16.
Reviewing update readiness results

After you run the Update Readiness tool, the tool returns test results in a log file. Table 1-4 lists the results summarized in the log file.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>Items that display under this section are confirmed and ready for update.</td>
</tr>
<tr>
<td>Warning</td>
<td>If not fixed, items that display under this section may prevent the database from upgrading properly.</td>
</tr>
<tr>
<td>Error</td>
<td>These items prevent the upgrade from completing and must be fixed.</td>
</tr>
</tbody>
</table>

See “Checking the database update readiness” on page 11.

About the minimum system requirements for upgrading to the current release

On Red Hat Enterprise Linux version 6.7 through 6.9 only, install the following additional packages before upgrading:

- Compat-openldap
- Compat-expat1
- Compat-db43
- openssl098e

On Red Hat Enterprise Linux version 7.1 through 7.3 only, install the following additional 64-bit packages before upgrading:

- Compat-openldap-1:2.3.43-5.el7
- compat-db47-4.7.25-28.e17
- libpng12
- Compat-libtiff3

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 that is 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: http://www.symantec.com/docs/DOC10602

See “About preparing to upgrade Symantec Data Loss Prevention” on page 8.

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 15.1, Endpoint Servers on version 14.6, and agents on version 14.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 15.1. You cannot upgrade either your Endpoint Servers or your agents before upgrading your Enforce Server.

Note: 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. 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 15.1. 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 15.1.

Note: If you are running DLP Agents on version 12.5.x, upgrade them to 14.6 before you upgrade detection servers to the latest Symantec Data Loss Prevention version. Version 12.5.x agents cannot communicate with version 15.1 detection servers.
## Supported upgrade backward compatibility for agents and servers

### Table 1-5  
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>15.1</td>
<td>15.1</td>
<td>15.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All incidents are sent to the Enforce Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy and configuration updates can be sent to the Endpoint Servers and agents.</td>
</tr>
<tr>
<td>15.1</td>
<td>15.1</td>
<td>15.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All incidents are sent to the Enforce Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy and configuration updates can be sent to the Endpoint Servers and agents.</td>
</tr>
</tbody>
</table>
### 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>15.1</td>
<td>15.1</td>
<td>14.6, 14.5, 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 can be sent to agents. However, new policy rules introduced in a given release are not supported by earlier agents; in general, new policy rules are supported by the same agent version in which the rule is introduced. <strong>Note:</strong> Version 12.5.x agents display on the Agent Overview screen. However, you cannot complete maintenance or troubleshooting steps for them, and policies and configuration settings cannot be sent to them and incidents are not received. Upgrade these agents to version 14.0 then to version 15.1.</td>
</tr>
</tbody>
</table>
## 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>15.1</td>
<td>15.0</td>
<td>14.6, 14.5, 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 can be sent to agents. However, new policy rules introduced in a given release are not supported by earlier agents; in general, new policy rules are supported by the same agent version in which the rule is introduced. <strong>Note:</strong> Version 12.5.x agents display on the Agent Overview screen. However, you cannot complete maintenance or troubleshooting steps for them, and policies and configuration settings cannot be sent to them and incidents are not received. Upgrade these agents to version 14.0 then to version 15.0.</td>
</tr>
</tbody>
</table>
### Table 1-5: 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>15.1</td>
<td>14.6</td>
<td>14.6</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>14.5</td>
<td>14.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14.0</td>
<td>14.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.5.x</td>
<td></td>
<td></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 8.

### 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 15.1. You cannot restart Network Discover scans until at least one Network Discover detection server has been upgraded to version 15.1.

- If a version 14.x or 15.0 detection server stops (shuts down) after you have upgraded the Enforce Server to version 15.1, you must upgrade that detection server to version 15.1 before it can restart.
After you upgrade the Enforce Server to version 15.1, 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 `SymantecDLPDetectionServerController` 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 8.

**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 are described in the following topics:

See “Upgrade requirements and restrictions” on page 21.

See "About external storage for incident attachments" on page 22.

See “Preparing the Oracle database for a Symantec Data Loss Prevention upgrade” on page 10.

See “Creating the Update Readiness tool database account” on page 13.

See “Creating the Enforce Reinstallation Resources file” on page 81.

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 16.

**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 a 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 `/DataLossPrevention/` 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 "SymantecDLP" user with the same password as your Enforce Server "SymantecDLP" 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 "SymantecDLP" user.
- If you are using a Microsoft Windows system for external storage, share the directory with Read/Write permissions with the external storage "SymantecDLP" 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 15.1, all new incident attachments are 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.
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
- Signing RPM files
- Migrating previous version data to a new Enforce Server installation
- Migrating a previous version detection server to the latest version
- Migrating previous version data to a new single-tier installation
- Verifying that the Enforce Server and the detection servers are running
- 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. See "Updating EDM indexes to the latest version" in the Symantec Data Loss Prevention Administration Guide or Updating EDM indexes to the latest version in the Help.

Table 2-1  Upgrading Symantec Data Loss Prevention

<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 “Downloading and extracting the upgrade software” on page 26.</td>
</tr>
<tr>
<td>2</td>
<td>Confirm that the Enforce Server and the detection servers are running.</td>
<td>See “Verifying that the Enforce Server and the detection servers are running” on page 42.</td>
</tr>
<tr>
<td>3</td>
<td>Close all files and folders in your opt/Symantec/DataLossPrevention/ directory.</td>
<td>Ensure that all folders and files in your DataLossPrevention directory are closed and unlocked. The upgrader requires access to all DataLossPrevention folders and files during the upgrade process.</td>
</tr>
<tr>
<td>5</td>
<td>Prepare and run the Update Readiness tool.</td>
<td>See “Creating the Update Readiness tool database account” on page 13.</td>
</tr>
<tr>
<td>6</td>
<td>Install the version 15.1 Enforce Server.</td>
<td>See “Installing an Enforce Server” on page 28.</td>
</tr>
<tr>
<td>7</td>
<td>Migrate the previous version to the version 15.1 Enforce Server.</td>
<td>See “Running the Migration Utility on the Enforce Server” on page 31.</td>
</tr>
<tr>
<td>8</td>
<td>Install the Java Runtime Environment on the detection server.</td>
<td>See “Installing the Java Runtime Environment on a detection server” on page 32.</td>
</tr>
<tr>
<td>9</td>
<td>Install the version 15.1 detection servers.</td>
<td>See “Installing a detection server” on page 33.</td>
</tr>
<tr>
<td>10</td>
<td>Migrate the previous version to the version 15.1 detection servers.</td>
<td>See “Running the Migration Utility on a detection server” on page 36.</td>
</tr>
</tbody>
</table>
Table 2-1  Upgrading Symantec Data Loss Prevention (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>(Optional) Apply the updated agent configuration to Endpoint Prevent detection servers.</td>
<td>See “Applying the updated configuration to Endpoint Prevent servers” on page 43.</td>
</tr>
<tr>
<td>12</td>
<td>(Optional) Update Symantec DLP Agents.</td>
<td>See “About Symantec Data Loss Prevention Agent upgrades” on page 44.</td>
</tr>
<tr>
<td>13</td>
<td>(Optional) Update any scanners.</td>
<td>See “Upgrading your scanners” on page 43.</td>
</tr>
<tr>
<td>14</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_15.1_Platform_Lin-IN.zip` file.
2. Extract the contents of the `Symantec_DLP_15.1_Agent_Win-IN.zip` file.
3. Extract the contents of the `Symantec_DLP_15.1_Agent_Mac-IN.zip` file.
4. Note where you saved the MSI and PKG files so you can quickly find them later.

See “Symantec Data Loss Prevention upgrade phases” on page 9.

### Signing RPM files

Before you install the latest Symantec Data Loss Prevention version, Symantec recommends that you use the RPM signing key to verify the signature of RPM files. All RPM packages provided in the `Symantec_DLP_15.1_Platform_Lin-IN.zip` are signed with a GPG key. The signature provides integrity protection and ensures that the packages are the same packages produced by Symantec and were not altered in any way by a malicious third-party.
Note: If you try to install and do not use the RPM signing key, a "NOKEY" warning message displays during the installation.

Use the RPM signing key before you install the Enforce Server, detection server, or a single-tier system.

To use the RPM signing key

1. Locate the Symantec_DLP_RPM_Signing_Key.asc file in the DLPDownloadHome directory. The Symantec_DLP_RPM_Signing_Key.asc is packaged in the Symantec_DLP_15.1_Platform_Lin-IN.zip file.

2. Copy the Symantec_DLP_RPM_Signing_Key.asc file to the computer where you plan to install the server component.

3. Log on as root to the computer where you plan to install the server component.

4. Import the key to the RPM key ring by running the following command:
   
rpm --import Symantec_DLP_RPM_Signing_Key.asc

5. Display the imported key by running the following command:
   
rpm -qi gpg-pubkey-b891399b-59c04bd7

6. Verify the signature of files before installing them by running the following command:
   
rpm -K *rpm

Migrating previous version data to a new Enforce Server installation

Upgrading the Enforce Server includes installing the new version where the existing version is running and migrating data to the new version.

To upgrade the Enforce Server to the latest version

1. Install the Java Runtime Environment on the Enforce Server.
   
   You can skip this step if you are already running a compatible JRE version.
   
   See “Installing the Java Runtime Environment on the Enforce Server” on page 28.

2. Run the Update Readiness tool.
   
   Ensure that the database is ready for the migration by running the Update Readiness Tool.
   
   See “Checking the database update readiness” on page 11.
3 Sign RPM files.
   See “Signing RPM files” on page 26.

4 Install the version 15.1 Enforce Server.
   You install the Enforce Server on the same system where the previous version is running.
   See “Installing an Enforce Server” on page 28.

5 Migrate the previous version to the version 15.1 Enforce Server.
   Migrating data—in addition to moving data to the new system—moves data, configurations,
   and custom files (which includes data profiles, plug-ins, and incidents) to the 15.1 instance.
   The migration utility also stops previous version services and starts new version services.
   See “Running the Migration Utility on the Enforce Server” on page 31.
   The process to migrate data does not move all plug-ins. See “Migrating plug-ins” on page 64.

Installing the Java Runtime Environment on the Enforce Server

You install the Java Runtime Environment (JRE) on the Enforce Server before you install the
Enforce Server.

---

**Note:** You can skip this step if you have already installed a JRE that meets Symantec Data Loss Prevention requirements.

---

To install the JRE

1 Copy `ServerJRE.zip` from your `DLPDownloadHome/DLP/New_Installs/Release` directory to the computer where you plan to install the Enforce Server.

2 Log on as root to the Enforce Server system on which you intend to install Enforce.

3 Unzip the file contents (for example, unzip to `/opt/temp`).

4 Install the JRE by running the following command:

   ```
   rpm -ivf symantec-dlp-server-jre-1-8-0-162-1.8.0.162-1.el6.x86_64.rpm
   ```

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server on a Linux computer.

These instructions assume that the `SymantecDLPEnforceServer.zip` file and license file have been copied into the `/opt/temp` directory on the Enforce Server computer.
To install an Enforce Server

1. Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.

2. Log on as root to the Enforce Server system on which you intend to install Enforce.

3. Navigate to the directory where you copied the SymantecDLPEnforceServer.zip file (/opt/temp/).

4. Unzip the file to the same directory (/opt/temp/).

5. Confirm file dependencies for RPM files by running the following command:
   
   ```sh
   rpm -qpR *.rpm
   ```
   
   You can also specify a file to confirm by running the following command:
   
   ```sh
   rpm -qpR .rpm-file
   ```

6. Install all RPM files in the folder by running the following command:
   
   ```sh
   rpm -ivf *.rpm
   ```
   
   You can also specify files to install by listing them in the command. For example, to install the Enforce Server and content extraction plug-ins, you run the following command:
   
   ```sh
   rpm -ivf symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
   symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
   ```
7 Or, use a non-default installation path of your choice as an alternative to step 6:

**Relocate the `/opt/Symantec/DataLossPrevention` directory**

```
rpm -ivh --relocate /opt/Symantec/DataLossPrevention=/opt/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-enforce-server-system-dependencies-1.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
```

**Relocate the `/var/Symantec/DataLossPrevention` directory**

```
rpm -ivh --relocate /var/Symantec/DataLossPrevention=/var/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
```

**Relocate the `/var/log/Symantec/DataLossPrevention` directory**

```
rpm -ivh --relocate /var/log/Symantec/DataLossPrevention=/var/log/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
```

**Relocate the `/var/run/Symantec/DataLossPrevention` directory**

```
rpm -ivh --relocate /var/run/Symantec/DataLossPrevention=/var/run/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
```

8 Navigate to the migrator directory: `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/Migrator`

9 Restart any antivirus, pop-up blocker, or other protection software that you disabled.

10 Run the Update Readiness tool to confirm that the Oracle database is ready to be migrated to the new instance, if you haven't run it already.

   See “Checking the database update readiness” on page 11.

11 Start the migration process.

   See “Running the Migration Utility on the Enforce Server” on page 31.
Running the Migration Utility on the Enforce Server

After you install the version 15.1 Enforce Server, you use the Migration Utility to migrate data to the new instance. Before you start the migration, use the Upgrade Readiness tool to confirm that the Oracle database is ready for migration.

Note: You must extract the Upgrade Readiness tool zip contents directly to the Enforce Server/15.1/Protect/Migrator/URT folder before you run the Migration Utility.

There are two ways to complete the migration; you can use silent mode or interactive mode. See “To migrate data from a previous Enforce Server version to version 15.1 using interactive mode ” on page 31.

The process to migrate data does not move all plug-ins. See “Migrating plug-ins” on page 64.

Note: Before you run the Migration Utility, you must switch to root user.

To migrate data from a previous Enforce Server version to version 15.1 using silent mode

- Use the following command to complete the migration using Silent Mode:

  ```
  ./EnforceServerMigrationUtility
  -silent
  -sourceInstallation="/opt/SymantecDLP"
  -jreDirectory="/opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162"
  ```

  Where "/opt/SymantecDLP" is the path to the previous version installation and "/opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162" points to the current JRE location.

To migrate data from a previous Enforce Server version to version 15.1 using interactive mode

1. Open the command prompt window.
2. Switch user to root: `su root`.
3. Go to the following directory:

   ```
   /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/Migrator
   ```

4. Run the Migration Utility by running the following command:

   ```
   ./EnforceServerMigrationUtility
   ```

   The Migration Utility stops services on the previous Symantec Data Loss Prevention version and migrates data, configuration, and custom files to the new version. When the process completes a message displays indicating that the migration has finished.
5 Select a version to migrate by entering 1.

Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.1 installation. If you uninstall the previous version, the service_user is removed.

6 Confirm the JRE directory that displays.

If no JRE displays, install the JRE.

See “Installing the Java Runtime Environment on the Enforce Server” on page 28.

7 If migration fails, review the Enforce Server migration logs in MigrationUtility.log located at /var/log/Symantec/DataLossPrevention/Enforce Server/15.1/debug/ for more details.

Migrating a previous version detection server to the latest version

Upgrading the detection server includes installing the new version where the existing version is running and migrating data to the new version.

To upgrade a detection server to the latest version

1 Install the Java Runtime Environment on the detection server.

You can skip this step if you are already running a compatible JRE version.

See “Installing the Java Runtime Environment on a detection server” on page 32.

2 Sign RPM files.

See “Signing RPM files” on page 26.

3 Install the version 15.1 detection servers.

See “Installing a detection server” on page 33.

4 Migrate the previous version to the version 15.1 detection servers.

See “Running the Migration Utility on a detection server” on page 36.

Installing the Java Runtime Environment on a detection server

You install the Java Runtime Environment (JRE) on the server computer before you install the detection server.
Note: You can skip this step if you have already installed a JRE that meets Symantec Data Loss Prevention requirements.

To install the JRE

1. Log on as root to the computer on which you intend to install the detection server.
2. Copy `SymantecDLPServerJRE.zip` from your 
   `DLPDownloadHome/DLP/New_Installs/Release` directory to the computer where you plan to install the detection server.
3. Unzip the file contents (for example, unzip to `/opt/temp`).
4. Install the JRE by running the following command:
   ```
   rpm -ivf symantec-dlp-server-jre-1-8-0-162-1.8.0.162-1.el6.x86_64.rpm
   ```

Installing a detection server

Follow this procedure to install the detection server software on a server computer. Note that you specify the type of detection server during the server registration process that follows this installation process.

Note: The following instructions assume that the `SymantecDLPDetectionServer.zip` file has been copied into the `/opt/temp/` directory on the server computer.

To install a detection server

1. Complete the preinstallation steps.
   See “About preparing to upgrade Symantec Data Loss Prevention” on page 8.
2. Log on as root to the computer on which you intend to install the detection server.
3. Copy the detection server installer (`SymantecDLPDetectionServer.zip`) from the Enforce Server to a local directory on the detection server. The `SymantecDLPDetectionServer.zip` file is included in your software download (`DLPDownloadHome`) directory. It should have been copied to a local directory on the Enforce Server during the Enforce Server installation process.
4. Navigate to the directory where you copied the `SymantecDLPDetectionServer.zip` file (`/opt/temp/`).
5. Unzip the file to the same directory.
6 Confirm file dependencies for RPM files by running the following command:

```
rpm -qRp *.rpm
```

You can also specify a file to confirm by running the following command:

```
rpm -qRp .rpm-file
```

where `.rpm-file` is the file you want to confirm.

7 Run the following command to install all RPM files in the folder:

```
rpm -ivf *.rpm
```

You can also specify files to install by listing them in the command. For example, to install the detection server and content extraction plug-ins, you run the following command:

```
rpm -ivf symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x84_64.rpm
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x84_64.rpm
```
8 Or, use the non-default installation path of your choice as an alternative to step 6.

Relocate the `/opt/Symantec/DataLossPrevention` directory:

```
rpm -ivh --relocate /opt/Symantec/DataLossPrevention=/opt/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.e16.x86_64.rpm
symantec-dlp-keyview-11-4-11.4.0.0-1.e16.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.e16.x86_64.rpm
```

Relocate the `/var/Symantec/DataLossPrevention` directory:

```
rpm -ivh --relocate /var/Symantec/DataLossPrevention=/var/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.e16.x86_64.rpm
```

Relocate the `/var/log/Symantec/DataLossPrevention` directory:

```
rpm -ivh --relocate /var/log/Symantec/DataLossPrevention=/var/log/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.e16.x86_64.rpm
```

Relocate the `/var/run/Symantec/DataLossPrevention` directory:

```
rpm -ivh --relocate /var/run/Symantec/DataLossPrevention=/var/run/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.e16.x86_64.rpm
```

Relocate the `/var/spool/Symantec/DataLossPrevention` directory:

```
rpm -ivh --relocate
/var/spool/Symantec/DataLossPrevention=/var/spool/Symc/DLP
```

```
symantec-dlp-15-1-content-extraction-service-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.e16.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.e16.x86_64.rpm
```

9 Navigate to the migrator directory: `/opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/Migrator`

10 Start the migration process.

See “Running the Migration Utility on a detection server” on page 36.
Running the Migration Utility on a detection server

After you install the version 15.1 detection server, you use the Migration Utility to migrate data to the new instance.

There are two ways to complete the migration. You can use silent mode or interactive mode. See “To migrate data from a previous Enforce Server version to version 15.1 using interactive mode” on page 36.

Note: Before you run the Migration Utility, you must switch to root user.

To migrate data from a previous Enforce Server version to version 15.1 using silent mode

- Use the following command to complete the migration using Silent Mode:

```
./DetectionServerMigrationUtility
-silent
-sourceInstallation="/opt/SymantecDLP"
-jreDirectory="/opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162"
```

Where "/opt/SymantecDLP" is the path to the previous version installation and /opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162 points to the current JRE location.

To migrate data from a previous Enforce Server version to version 15.1 using interactive mode

1. Open the command prompt window.
2. Switch user to root: su root.
3. Go to the following directory:

```
/opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/Migrator
```
4. Run the Migration Utility by running the following command:

```
./DetectionServerMigrationUtility
```

The Migration Utility stops services on the previous detection server version and migrates data, configuration, and custom files to the new version. When the process completes a message displays indicating that the migration has finished.

5. Select a version to migrate by entering 1.

Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.1 installation. If you uninstall the previous version, the service_user is removed.
6 Confirm the JRE directory that displays.  
If no JRE displays, install the JRE.  
See “Installing the Java Runtime Environment on a detection server” on page 32.

7 If migration fails, review the detection server migration logs in MigrationUtility.log located at /var/log/Symantec/DataLossPrevention/Detection Server/15.1/debug/.  
The process to migrate data does not move all plug-ins. See “Migrating plug-ins” on page 64.

Migrating previous version data to a new single-tier installation

After you install the version 15.1 single-tier system, you use the Migration Utility to migrate data to the new instance. Before you run the Migration Utility, run the Update Readiness tool to confirm that the database is ready for migration.  
See “Checking the database update readiness” on page 11.

To upgrade a single-tier installation to the latest version

1 Install the Java Runtime Environment on the Enforce Server.  
You can skip this step if you are already running a compatible JRE version.  
See “Installing the Java Runtime Environment on the Enforce Server” on page 28.

2 Run the Update Readiness tool.  
Running the tool identifies potential issues with the database.  
See “Creating the Update Readiness tool database account” on page 13.

3 Sign RPM files.  
See “Signing RPM files” on page 26.

4 Install the version 15.1 single-tier system.  
You install the single-tier system on the same computer where the previous version is running.  
See “Installing a single-tier server” on page 38.

5 Migrate the previous version to the version 15.1 single-tier installation.  
See “Running the Migration Utility on single-tier installation” on page 41.

Installing the Java Runtime Environment for a single-tier installation

You install the Java Runtime Environment (JRE) before you complete a single-tier installation.
Note: You can skip this step if you have already installed a JRE that meets Symantec Data Loss Prevention requirements.

To install the JRE

1. Copy SymantecDLPServerJRE.zip to the computer where you plan to install the single-tier system.
2. Log on as root to the computer where you plan to install the single-tier system.
3. Unzip the file contents (for example, unzip to opt\temp).
4. Install the JRE by running the following command:
   
   ```
   rpm -ivf symantec-dlp-server-jre-1-8-0-162-1.8.0.162-1.el6.x86_64.rpm
   ```

Installing a single-tier server

Symantec recommends that you disable any antivirus, pop-up blocker, and registry-protection software before you begin the Symantec Data Loss Prevention installation process.

Note: The following instructions assume that the SymantecDLPSingleTierServer.zip file, license file, and solution pack file have been copied into the /opt/temp directory on the Symantec Data Loss Prevention single-tier installation server.

To install the single-tier server

1. Log on as root to the computer that is intended for the Symantec Data Loss Prevention single-tier installation.
2. Copy the Symantec Data Loss Prevention single-tier installer (SymantecDLPSingleTierServer.zip) from DLPDownloadHome to a local directory on the single-tier computer (for example, /opt/temp/).
3. Unzip the file to the same directory (/opt/temp/).
4. Confirm file dependencies for RPM files by running the following command:

   ```
   rpm -qP *.rpm
   ```

5. Run the following command to install all RPM files in the folder:

   ```
   rpm -ivf *.rpm
   ```
You can also specify files to install by listing them in the command. For example, to install a single-tier server, you run the following command:

```
rpm -ivf symantec-dlp-15-1-single-tier-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-enforce-server-system-dependencies-1.0.0-1.el6.x86_64.rpm
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x84_64.rpm
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x84_64.rpm
```
7 Or use a non-default installation path of your choice as an alternative to step 6.

Relocate the /opt/Symantec/DataLossPrevention directory:

```
rpm -ivh --relocate /opt/Symantec/DataLossPrevention=/opt/Symc/DLP
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-enforce-server-system-dependencies-1.0.0-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
```

Relocate the /var/Symantec/DataLossPrevention directory:

```
rpm -ivh --relocate /var/Symantec/DataLossPrevention=/var/Symc/DLP
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
```

Relocate the /var/log/Symantec/DataLossPrevention directory:

```
rpm -ivh --relocate /var/log/Symantec/DataLossPrevention=/var/log/Symc/DLP
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
```

Relocate the /var/run/Symantec/DataLossPrevention directory:

```
rpm -ivh --relocate /var/run/Symantec/DataLossPrevention=/var/run/Symc/DLP
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
```

Relocate the /var/spool/Symantec/DataLossPrevention directory:

```
rpm -ivh --relocate
/var/spool/Symantec/DataLossPrevention=/var/spool/Symc/DLP
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x86_64.rpm
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64.rpm
```

8 Navigate to the migrator directory. The default directory is

```
/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/migrator
```
9 Restart any antivirus, pop-up blocker, or other protection software that you disabled.

10 If you have not done so already, run the Update Readiness tool to confirm that the Oracle database is ready to be migrated to the new instance. If you have already run the Upgrade Readiness tool, skip this step.
   
   See “Checking the database update readiness” on page 11.

11 Start the migration process.

12 See “Running the Migration Utility on single-tier installation” on page 41.

Running the Migration Utility on single-tier installation

After you install the version 15.1 single-tier system, you can migrate data using the Migration Utility. Before you start the migration, use the Upgrade Readiness tool to confirm that the Oracle database is ready for migration.

The process to migrate data does not move all plug-ins. See “Migrating plug-ins” on page 64.

Note: You must extract the Upgrade Readiness tool zip contents directly to the Enforce Server/15.1/Protect/Migrator/URT folder before you run the Migration Utility.

You can use one of two ways to complete the migration: silent mode or interactive mode.

See “To migrate data from a previous single-tier version to version 15.1 using interactive mode” on page 41.

Note: Before you run the Migration Utility, you must switch to root user.

To migrate data from a previous single-tier version to version 15.1 using silent mode

◆ Use the following command to complete the migration using silent mode:

```
./SingleTierServerMigrationUtility
-silent
-sourceInstallation="/opt/SymantecDLP"
-jreDirectory="/opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162"
```

Where "/opt/SymantecDLP" is the path to the previous version installation and "/opt/Symantec/DataLossPrevention/Server JRE/1.8.0_162" points to the current JRE location.

To migrate data from a previous single-tier version to version 15.1 using interactive mode

1 Open the command prompt window.

2 Switch to root user: su root.
3 Go to the following directory:
   /opt/Symantec/DataLossPrevention/Single Tier Server/15.1/Protect/Migrator

4 Run the Migration Utility using the following command:
   ./SingleTierServerMigrationUtility

5 The Migration Utility stops services on the previous version single-tier system and migrates data, configuration, and custom files to the new version. When the process completes a message displays indicating that the migration has finished.

6 Select a version to migrate by entering 1.

---

Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.1 installation.

---

7 Confirm the JRE directory that displays.
   If no JRE displays, install the JRE.
   See “Installing the Java Runtime Environment for a single-tier installation” on page 37.

8 If the migration fails, review the single-tier server migration logs on MigrationUtility.log located at /var/log/Symantec/DataLossPrevention/Single Tier Server/15.1/debug/.

---

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 are running the appropriate Symantec Data Loss Prevention services.
See “About Symantec Data Loss Prevention services” on page 73.

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.
See “Upgrading Symantec Data Loss Prevention” on page 24.
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 15.1 scanners. To upgrade a scanner, remove the older software and then install the Symantec Data Loss Prevention 15.1 scanner.

See the **Symantec Data Loss Prevention Administration Guide** for information on adding and removing scanners: [http://www.symantec.com/docs/DOC9261](http://www.symantec.com/docs/DOC9261)

See “Symantec Data Loss Prevention upgrade phases” on page 9.

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: [http://www.symantec.com/docs/DOC9261](http://www.symantec.com/docs/DOC9261)
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 12.x DLP Agent with a 15.1 Endpoint Server. Endpoint Servers are backward-compatible with a DLP Agent for one full release. For example, a version 15.1 Endpoint Server and a version 14.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 45.</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 56.</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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrading the Windows agent silently” on page 54.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrading DLP Agents on Mac endpoints silently” on page 60.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Upgrade the DLP Agent manually.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrading the Windows agent manually” on page 53.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrading the DLP Agent for Mac manually” on page 59.</td>
</tr>
</tbody>
</table>

About secure communications between DLP Agents and Endpoint Servers

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

Symantec Data Loss Prevention sets up a root Certificate Authority (CA) 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 Symantec Data Loss Prevention CA.
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.

See “Generating agent installation packages” on page 46.

Generating agent installation packages

You use the System > Agents > Agent Packaging screen to generate the installation package for DLP Agents. You can use the screen to create an installation package that includes—in addition to the DLP Agent—the ICT Client and ICE Utility.

See “About secure communications between DLP Agents and Endpoint Servers” on page 45.

The packaging process creates a zip file that contains the installer of your choosing. The zip file includes public certificate and keys and installation scripts to install DLP Agents, ICT Clients, and ICE Utilities. You generate a single installation package for each endpoint platform where you want to deploy.

For example, if you want to install DLP Agents, ICT Clients, and ICE Utilities 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.

Before you start generating the agent installation packages confirm that your system is ready to package by completing the following:

- Confirm that the agent installers are copied to the Enforce Server local file system. See “Downloading and extracting the upgrade software” on page 26.
- Confirm that the Enforce Server has at least 3 GB of free space. The packaging process fails if the Enforce Server has less than 3 GB of free space.

Table 3-2 provides instructions for generating agent installation packages. The instructions assume that 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 Agent Packaging page.</td>
<td>Log on to the Enforce Server administration console as an administrator and navigate to the System &gt; Agents &gt; Agent Packaging page.</td>
</tr>
</tbody>
</table>
### Table 3-2  Generating the agent installation package (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2    | Select the agent version. | Select an item in the **Select the agent version** list that matches the agent installer files you plan to package. You can select one of the following:  
- **Pre-version 15.0**  
  Applies to agent versions 12.5.x through 14.6.x.  
- **Version 15.0**  
  Applies to agent version 15.0.x.  
- **Version 15.1 and later**  
  Applies to all agent versions starting with 15.1.  
You must select 32- and 64-bit installation files that match the agent version you selected. For example, selecting a version 15.0 32-bit and a version 15.1 64-bit installation file while selecting **Version 15.1 and later** in the list is unsupported. Selecting mis-matched versions prevents agents from installing on endpoints.  
If you plan to package an ICT Client and ICE Utility with the DLP agent, you must select **Version 15.1 and later**. |
| 3    | 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** AgentInstallers-x64_15_1.zip  
**Windows 32-bit** AgentInstallers-x86_15_1.zip |
| 4    | 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. |
| 5    | 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. |
### Table 3-2 Generating the agent installation package (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6    | Add additional servers (optional). | Click the plus sign to add additional servers for failover.  
**Note:** Symantec Data Loss Prevention allots 2048 characters for Endpoint Server names. This allotment includes the characters that are used for the Endpoint Server name, port numbers, and semicolons to delimit each server.  
The first server that is listed is the primary; additional servers are secondary and provide backup if the primary is down. |
| 7    | 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. You should store this password in a secure format of your own so that it can be retrieved if forgotten.  
After installing agents, you can change the password on the **Agent Password Management** screen. |
| 8    | Re-enter the Endpoint tools password. | The system validates that the passwords match and displays a message if they do not. |
| 9    | Enter the target directory for the agent installation (Windows only). | 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 using English characters. Using non-English characters can prevent the DLP Agent from starting and from monitoring data in some scenarios.  
**Note:** 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. |
| 10   | Enter the uninstall password (optional, Windows only). | The agent uninstall password is supported for Windows agents. The uninstall password is a tamper-proof mechanism that requires a password to uninstall the DLP Agent.  
The password is encrypted and stored in a file on the Enforce Server. You should store this password in a secure format of your own so that it can be retrieved if forgotten.  
After installing agents, you can change the password on the **Agent Password Management** screen. |
### Table 3-2 Generating the agent installation package (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Re-enter the uninstall password.</td>
<td>The system validates that the passwords match and displays a message if they do not.</td>
</tr>
</tbody>
</table>
| 12   | (Optional) Select Install the Symantec ICT Client. | Select this option to package the ICT Client with the agent package. Enter the License and ICT Web Service URL. Go to the Information Centric Tagging Administration Console to gather information for the following fields:  
- **License**  
  After the ICT admin installs the ICT server and uploads a license file on the Server Keys tab, a server public key displays. Enter that key in the License field.  
- **ICT Web Service URL**  
  The ICT admin defines this URL on the Encryption tab, in the URL of Rights Template Manager Web Services field. Enter that URL in the ICT Web Service URL field.  
  For more information about these two fields, see the Symantec Information Centric Tagging Deployment Guide:  
  [http://www.symantec.com/docs/DOC11006](http://www.symantec.com/docs/DOC11006) |
| 13   | (Optional) Select Install the Symantec ICE Utility. | Select this option to package the ICE Utility with the agent package. For more information about the ICE Utility, see the Symantec Information Centric Encryption Deployment Guide:  
[http://www.symantec.com/docs/DOC9707](http://www.symantec.com/docs/DOC9707) |
| 14   | Click Generate Installer Packages. | This action generates the agent installer package for each platform that you selected in step 3. The generation process may take a few minutes. |
Table 3-2  Generating the agent installation package (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</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. After you save the file you can navigate away from the Agent Packaging screen to complete the process. The zip file is named according 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. In this case, the zip file contains separate zip files for each agent package for each platform you selected in step 23. See “Agent installation package contents” on page 50.</td>
</tr>
<tr>
<td>16</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 46.

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-x86_15_1.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></td>
</tr>
<tr>
<td>endpoint_truststore.pem</td>
<td>See “Working with endpoint certificates” on page 52.</td>
</tr>
</tbody>
</table>
Table 3-3  
**AgentInstaller_Win32.zip and AgentInstaller_Win64.zip installation package contents (continued)**

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSEndpoint-x64_15_1.exe</td>
<td>Use to install the ICT Client and ICE Utility.</td>
</tr>
<tr>
<td>install_agent.bat</td>
<td>Use to install the DLP Agent, ICT Client, and ICE Utility silently.</td>
</tr>
<tr>
<td>rw-config.ini</td>
<td>Use to install the ICT Client silently.</td>
</tr>
<tr>
<td></td>
<td>For additional details on this file, refer to the Symantec Information Centric Tagging Deployment Guide: <a href="http://www.symantec.com/docs/DOC11006">http://www.symantec.com/docs/DOC11006</a></td>
</tr>
<tr>
<td>upgrade_agent.bat</td>
<td>Use to upgrade the DLP Agent, ICT Client, and ICE Utility silently.</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 macOS.

Table 3-4  
**AgentInstaller_Mac64.zip installation package contents**

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentInstall_15_1.pkg</td>
<td>Mac DLP Agent installer</td>
</tr>
<tr>
<td>AgentInstall.plist</td>
<td>Mac DLP Agent installation properties configuration file</td>
</tr>
<tr>
<td>create_package</td>
<td>Use to generate the DLP Agent installation package for macOS. You can use this package to install agents manually or use 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 52.</td>
</tr>
<tr>
<td>endpoint_truststore.pem</td>
<td></td>
</tr>
<tr>
<td>ICE_Managed_OSX.pkg</td>
<td>ICE client installer</td>
</tr>
<tr>
<td>install_agent.sh</td>
<td>Use to install the DLP Agent and the ICE Utility.</td>
</tr>
<tr>
<td>Install_Readme.rtf</td>
<td>Provides commands for packaging and installing the agent</td>
</tr>
<tr>
<td></td>
<td>See “Process to upgrade the DLP Agent on Mac” on page 56.</td>
</tr>
</tbody>
</table>
Working with endpoint certificates

Symantec Data Loss Prevention automatically generates the public certificates and the keys needed for authentication and secure communications between DLP Agents and Endpoint Server. The public certificates and keys are securely stored in the Enforce Server database. See “About secure communications between DLP Agents and Endpoint Servers” on page 45.

When you install or upgrade the Enforce Server, the system generates the DLP root certificate authority (CA). 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 46.

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 44.

Table 3-5  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 “Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled” on page 53.</td>
</tr>
</tbody>
</table>
Table 3-5  Process to upgrade agents on Windows endpoints (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Upgrade the agent.</td>
<td>See “Upgrading the Windows agent manually” on page 53.</td>
</tr>
<tr>
<td></td>
<td>Upgrade an agent manually. You can upgrade an agent manually when you</td>
<td>See “Upgrading the Windows agent silently” on page 54.</td>
</tr>
<tr>
<td></td>
<td>want to test the configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade the agents using your SMS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You upgrade agents using this method to upgrade many agents at one time.</td>
<td></td>
</tr>
</tbody>
</table>

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 15.1, 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 46.
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 46.
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="epserv: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</td>
<td>Properties for the agent installation package.</td>
</tr>
<tr>
<td>SERVICENAME</td>
<td>Properties that reference the files and the passwords that are associated with the agent certificates.</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td></td>
</tr>
<tr>
<td>UNINSTALLPASSWORDKEY</td>
<td></td>
</tr>
<tr>
<td>WATCHDOGNAME</td>
<td></td>
</tr>
<tr>
<td>TOOLS_KEY</td>
<td></td>
</tr>
<tr>
<td>ENDPOINT_CERTIFICATE</td>
<td></td>
</tr>
<tr>
<td>ENDPOINT_PRIVATEKEY</td>
<td></td>
</tr>
<tr>
<td>ENDPOINT_TRUSTSTORE</td>
<td></td>
</tr>
<tr>
<td>ENDPOINT_PRIVATEKEY_PASSWORD</td>
<td></td>
</tr>
<tr>
<td>VERIFY_SERVER_HOSTNAME</td>
<td></td>
</tr>
<tr>
<td>STARTSERVICE</td>
<td></td>
</tr>
<tr>
<td>ENABLEWATCHDOG</td>
<td></td>
</tr>
<tr>
<td>LOGDETAILS</td>
<td></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\15.1\Endpoint\x64\install_agent64.bat or
DLPDownloadHome\DLP\15.1\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 44.

**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 44.

**Table 3-6**  
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 57.</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 59. See “Upgrading DLP Agents on Mac endpoints silently” on page 60.</td>
</tr>
</tbody>
</table>
Table 3-6  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 61.</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 61.</td>
</tr>
<tr>
<td></td>
<td>These components include the drivers that prevent tampering and keep 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 45.
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 50.

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 59.

   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.

   See “Upgrading DLP Agents on Mac endpoints silently” on page 60.
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_15.1_Agent_Mac-IN.zip file.
- Maintenance tools are found in the SymantecDLPMacAgentTools_15.1.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 57.

Table 3-7 lists the available tools.

<table>
<thead>
<tr>
<th>Tool type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>agent.ver adds agent package versioning information.</td>
</tr>
<tr>
<td></td>
<td>start_agent restarts the Mac agents that have been</td>
</tr>
<tr>
<td></td>
<td>shut down on the Agent List screen.</td>
</tr>
<tr>
<td></td>
<td>uninstall_agent uninstalls the DLP Agent from Mac</td>
</tr>
<tr>
<td></td>
<td>endpoints.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>vontu_sqlite3 lets you inspect the agent database.</td>
</tr>
<tr>
<td></td>
<td>logdump creates agent log files.</td>
</tr>
</tbody>
</table>

Upgrading the DLP Agent for Mac manually

Table 3-8 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 60.

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 45.
### 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_15_1.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_15_1.pkg -target / -dumplog.  
Replace /tmp/MacInstaller with the path where you unzipped the agent installation package. |

### 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 46.

See "Packaging Mac agent upgrade files" on page 57.

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 `install.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 61.

---

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 3-9  Mac agent components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Agent daemon (EDPA)</td>
<td>The installation process places the EDPA files here: <code>/Library/Manufacturer/Endpoint Agent</code>. The <code>com.symantec.manufacturer.agent.plist</code> file contains configuration settings for the Endpoint Agent daemon. This file is located at <code>/Library/LaunchDaemons/</code>.</td>
</tr>
<tr>
<td>Encrypted database</td>
<td>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.</td>
</tr>
<tr>
<td>Log files</td>
<td>The DLP Agent logs information on completed and failed processes.</td>
</tr>
<tr>
<td>Database (<code>rrc.ead</code>)</td>
<td>This database maintains and contains non-matching entries for rules results caching (RRC).</td>
</tr>
</tbody>
</table>
Post-upgrade tasks

This chapter includes the following topics:

- Performing post-upgrade tasks
- Verifying Symantec Data Loss Prevention operations
- Migrating plug-ins
- About securing communications between the Enforce Server and the database

Performing post-upgrade tasks

You must perform certain tasks after you finish upgrading.

See “Verifying Symantec Data Loss Prevention operations” on page 63.
See “Symantec Data Loss Prevention upgrade phases” on page 9.

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 current version 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*.

---

**Migrating plug-ins**

During the upgrade process, the Migration Utility moves plug-ins from the previous version system to the new system location: `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/plugins`. Specifically, the following plug-ins are migrated:

- FileShare\plugin_settings
- MicrosoftRightsManagementPlugin\rightsManagementConfiguration
- MicrosoftRightsManagementPlugin\rightsManagementConfigurationProtection
- contentextraction\MarkupTestPlugin

The Migration Utility does not move plug-ins in other locations, previous version log files, or JAR file to the new version system location. You manually copy plug-ins to the new location.

**To migrate remaining plug-ins**

1 Locate plug-ins you plan to move.

   Most previous version plug-ins are stored at `opt/SymantecDLP/Protect/plugins` on the previous version system.

2 Copy plug-ins to the following locations on the new version system:

   - **Enforce Server**: `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/plugins`
   - **Detection server**: `/opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/plugins`
About securing communications between the Enforce Server and the database

You can use Transport Layer Security (TLS) to encrypt all data that is transmitted between the Enforce Server and the database server in a three-tier environment. You create unique, self-signed certificates that you store on the Enforce Server.

You must upgrade Symantec Data Loss Prevention before you secure communications between the Enforce Server and the database using TLS. The Symantec Data Loss Prevention upgrade cannot communicate over TLS. See “Upgrading Symantec Data Loss Prevention” on page 24.

Table 4-1 describes the process to secure communications between the Enforce Server and the database.

Table 4-1  Steps to secure communications between the Enforce Server and the database

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>More info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate the self-signed certificates using the orapki command-line utility that is provided with the Oracle database.</td>
<td>See “About orapki command line options” on page 65. See “Using orapki to generate the server certificate on the Oracle database” on page 66.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the JDBC driver on the Enforce Server to use the TLS connection and port.</td>
<td>See “Configuring communication on the Enforce Server” on page 68.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the server certificate on the Enforce Server.</td>
<td>See “Configuring the server certificate on the Enforce Server” on page 70.</td>
</tr>
</tbody>
</table>

About orapki command line options

You use the orapki command-line utility to create a wallet where certificates are stored. You then use the utility to generate a unique pair of TLS self-signed certificates that are used to secure communication between the Enforce Server and the Oracle database.

The orapki utility can be found in the $ORACLE_HOME/bin folder where the Oracle database is located. You run the orapki utility on the computer where the Oracle database is located.

Table 4-2 lists the command forms and options that you use when generating a unique pair of TLS self-signed certificates.
### Orapki utility examples

<table>
<thead>
<tr>
<th>Command and options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>orapki wallet create</strong> -wallet ./server_wallet -auto_login -pwd password</td>
<td>You use this command to create a wallet where certificates are stored. This command also creates the <code>server_wallet</code> directory.</td>
</tr>
<tr>
<td><strong>orapki wallet add</strong> -wallet /opt/oracle/wallet/server_wallet -dn &quot;CN=oracleserver&quot; -keysize 2048 -self_signed -validity 3650 -pwd password -sign_alg sha256</td>
<td>You use this command to add a self-signed certificate and a pair of private/public keys to the wallet.</td>
</tr>
<tr>
<td><strong>orapki wallet display</strong> -wallet /opt/oracle/wallet/server_wallet</td>
<td>You use this command to view the contents of the wallet to confirm that the self-signed certificate was created successfully.</td>
</tr>
<tr>
<td><strong>orapki wallet export</strong> -wallet /opt/oracle/wallet/server_wallet -dn &quot;CN=oracleserver&quot; -cert /opt/oracle/wallet/server_wallet/cert.txt</td>
<td>You use this command to export the self-signed certificate. In addition to exporting the certificate files, the command creates the file <code>cert.txt</code> in the <code>./server_wallet</code> directory.</td>
</tr>
</tbody>
</table>

### Using orapki to generate the server certificate on the Oracle database

Complete the following steps to generate the server certificate on the Oracle database.

**To generate certificates**

1. **Stop the Oracle database.**
   - To stop the database, run the following command as a root user:
     ```bash
     $ sh /etc/init.d/dbora stop
     ```

2. **Log on as the Oracle User by running the following command:**
   ```bash
   su - oracle
   ```

3. **Go to the `oracle` directory by running the following command:**
   ```bash
   cd /opt/oracle
   ```

4. **Create the wallet directory by running the following command:**
   ```bash
   mkdir wallet
cd wallet
   ```
5 Create a wallet on the Oracle server with auto login enabled by running the following command in the /opt/oracle/wallet directory:

```
orapki wallet create -wallet ./server_wallet -auto_login -pwd walletpassword
```

**Note:** Use a wallet password that adheres to the password policy. Passwords must have a minimum length of eight characters and contain alphabetic characters combined with numbers or special characters.

On Oracle 12c systems, the **Operation is successfully completed** message displays when the command completes. The following two files are created under the `server_wallet` directory (among similarly named `.lck` files):

- `cwallet.sso`
- `ewallet.p12`

6 Generate the self-signed certificate and add it to the wallet by running the following command:

```
orapki wallet add -wallet /opt/oracle/wallet/server_wallet -dn "CN=oracleserver" -keysize 2048 -self_signed -validity 3650 -pwd walletpassword -sign_alg sha256
```

Replace `oracleserver` with the name of the computer where Oracle is running.

7 View the wallet to confirm that the certificate was created successfully by running the following command:

```
orapki wallet display -wallet /opt/oracle/wallet/server_wallet
```

When the certificate is created successfully, the command returns information in the following form:

**Requested Certificates:**

**User Certificates:**

Subject: CN=oracleserver

**Trusted Certificates:**

Subject: CN=oracleserver

8 Export the certificate by running the following command:

```
orapki wallet export -wallet /opt/oracle/wallet/server_wallet -dn "CN=oracleserver" -cert /opt/oracle/wallet/server_wallet/cert.txt
```

9 Confirm that `cert.txt` is created at the following location:

```
/opt/oracle/wallet/server_wallet
```
Configuring communication on the Enforce Server

After you generate the server certificate on the Oracle database, you update the `listener.ora` file to point to the self-signed certificate.

To configure the JDBC driver on the Enforce Server

1. Back up the `listener.ora` file before you update it.
   
   The file is located at `$ORACLE_HOME/network/admin`.

2. Switch to the Oracle user by running the following command:
   
   `su - oracle`

3. Stop the listener by running the following command:
   
   `lsnrctl stop`
   
   You can skip this step if the database is already stopped.

4. Open the `listener.ora` file.

5. Update the port number to 2484 and the protocol to `TCPS` on the `Address` line.
   
   The `Listener` section should read as follows:

   ```
   LISTENER =
   (DESCRIPTION_LIST =
   (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCPS)(HOST = [oracle host name])(PORT = 2484))
    (ADDRESS = (PROTOCOL = IPC)(KEY = protect))
   )
   )
   ```

6. Add the following section to follow the `Listener` section:

   ```
   Note: Confirm that the directory points to the server_wallet location.
   ```

   ```
   SSL_CLIENT_AUTHENTICATION = FALSE
   WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY = /opt/oracle/wallet/server_wallet)))
   ```

7. Navigate to the directory `$ORACLE_HOME/network/admin` and open the `sqlnet.ora` file.
   Create a new `sqlnet.ora` file if it does not exist.
Replace the line `SQLNET.AUTHENTICATION_SERVICES=(TNS)` with the following:

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY = /opt/oracle/wallet/server_wallet)))
```

Navigate to the directory `$ORACLE_HOME/network/admin` and open the `tnsnames.ora` file.

Update the protocol to `TCPS` and the port to `2484`. The updated content should match the following:

```
PROTECT =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCPS) (HOST = [oracle host name]) (PORT = 2484))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = protect)
    )
  )

LISTENER_PROTECT =
  (ADDRESS = (PROTOCOL = TCPS) (HOST = [oracle host name]) (PORT = 2484))
```

If you are running the Oracle 11g database, you must run the following command to relink necessary files:

```
$ cd $ORACLE_HOME/lib
$ cp libntcps11.a libntcps11.a.orig
$ cp libntcps11_ee.a.db1 libntcps11.a
$ relink all
```
Start the Oracle database by running the following command:

```sh
$ sh /etc/init.d/dbora start
```

Confirm that the Oracle listener is operating by running the following command:

```bash
lsnrctl status
```

The listener status displays in the command prompt.

If the command prompt indicates that the listener is running but no services are running on the database, run the following commands:

```bash
su - oracle
export ORACLE_SID=protect
sqlplus /nolog
SQL> conn sys/<password> as sysdba
```

If **Connected to an idle instance** displays, run the following command:

```sql
SQL> startup
SQL> exit
lsnrctl status
```

### Configuring the server certificate on the Enforce Server

After you configure communication on the Enforce Server, you configure the JDBC driver and the server certificate. You configure the JDBC driver to use the TLS connection and port, then you configure the server certificate.

**To configure the server certificate on the Enforce Server**

1. Locate the `jdbc.properties` file located at `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/protect/config`.

2. Modify the following communication port and connection information:
   - Update the `jdbc.dbalias.oracle-thin` line to use **TCPS**.
   - Change the port number to **2484**.

The updated communication port and connection information should display as follows:

```java
jdbc.dbalias.oracle-thin@(description=(address=(host=[oracle host name])(protocol=tcps)(port=2484))(connect_data=(sid=protect))(SSL_SERVER_CERT_DN="CN=oracleserver"))
```
3 Add the certificate to the `cacerts` file that is located on the Enforce Server by completing the following steps:

**Note:** If the server certificate on the Oracle database is signed by a public CA (instead of being self-signed), skip to 4.

a  Copy the `cert.txt` file to
    `/opt/Symantec/DataLossPrevention/jre/lib/security`
    See "Using orapki to generate the server certificate on the Oracle database" on page 66.

b  Change the directory by running the following command:
    `cd /opt/Symantec/DataLossPrevention/jre/lib/security/`

c  Insert the certificate into the `cacerts` file by running the following command as a root user:
    `keytool -import -alias oracleservercert -keystore cacerts -file cert.txt`
    Enter the default password when you are prompted: **changeit**.

d  Confirm that the certificate was added by running the following command:
    `keytool -list -v -keystore /opt/Symantec/DataLossPrevention/jre/lib/security/cacerts -storepass changeit`

4 Restart all SymantecDLP services.

**Verifying the Enforce Server-database certificate usage**

To confirm that certificates are configured correctly and the Enforce Server is communicating with the database, log on to the Enforce Server administration console. If you can log on, the Enforce Server and database are communicating over a secure communication.

If you cannot log on, confirm the SSL Java application connection. To confirm the SSL Java application connection, check the listener status on the database server. In the listener status, the TCPS protocol and port 2484 should be in use. If the listener status does not display these connection statuses, re-complete the process to generate the self-signed certificates.

For full details on how to configure secure sockets layer authentication, see the following platform-specific documentation from Oracle Corporation, available from the Oracle Documentation Library:

Oracle 12c SE2: [https://docs.oracle.com/database/121/DBSEG/asossl.htm#DBSEG070](https://docs.oracle.com/database/121/DBSEG/asossl.htm#DBSEG070)
See "About securing communications between the Enforce Server and the database" on page 65.
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>Symantec DLP Manager</td>
<td>Provides the centralized reporting and management services for Symantec Data Loss Prevention.</td>
</tr>
<tr>
<td></td>
<td>If you have more than 50 policies, 50 detection servers, or 50,000 agents,</td>
</tr>
<tr>
<td></td>
<td>increase the Max Memory for this service from 2048 to 4096. You can adjust this setting in the SymantecDLPManager.conf file.</td>
</tr>
<tr>
<td></td>
<td>See &quot;To increase memory for the Symantec DLP Manager service&quot; on page 74.</td>
</tr>
</tbody>
</table>
Table 5-1  Symantec Data Loss Prevention services (continued)

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec DLP Detection Server Controller</td>
<td>Controls the detection servers. If you have more than 50 policies, 50 detection servers, or 50,000 agents, increase the Max Memory for this service from 1024 to 2048. You can adjust this setting in the SymantecDLPDetectionServerController.conf file. See “To increase memory for the Symantec DLP Detection Server Controller service” on page 74.</td>
</tr>
<tr>
<td>Symantec DLP Notifier</td>
<td>Provides the database notifications.</td>
</tr>
<tr>
<td>Symantec DLP Incident Persister</td>
<td>Writes the incidents to the database.</td>
</tr>
</tbody>
</table>

To increase memory for the Symantec DLP Manager service

1. Open the SymantecDLPManager.conf file in a text editor. You can find this configuration file in one of the following locations:
   - Windows: \Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\services
   - Linux: /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/services

2. Change the value of the wrapper.java.maxmemory parameter to 4096.

   wrapper.java.maxmemory = 4096

3. Save and close the file.

To increase memory for the Symantec DLP Detection Server Controller service

1. Open the SymantecDLPDetectionServerController.conf file in a text editor. You can find this configuration file in one of the following locations:
   - Windows: \Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\services
Starting and stopping Symantec Data Loss Prevention services

About Symantec Data Loss Prevention services

Linux: /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/services

2 Change the value of the wrapper.java.maxmemory parameter to 2048.

wrapper.java.maxmemory = 2048

3 Save and close the file.

Starting and stopping services on Linux

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

- See "Starting an Enforce Server on Linux" on page 75.
- See “Stopping an Enforce Server on Linux” on page 76.
- See “Starting a detection server on Linux” on page 76.
- See “Stopping a detection server on Linux” on page 76.
- See “Starting services on single-tier Linux installations” on page 77.
- See “Stopping services on single-tier Linux installations” on page 77.

Starting an Enforce Server on Linux

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

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

1 On the computer that hosts the Enforce Server, log on as root.

2 Start the Symantec DLP Notifier service by running the following command:

   service SymantecDLPNotifier start

3 Start the remaining Symantec Data Loss Prevention services, by running the following command:

   service SymantecDLPManager start
   service SymantecDLPIncidentPersister start
   service SymantecDLPDetectionServerController start

See “Stopping an Enforce Server on Linux” on page 76.
Stopping an Enforce Server on Linux

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

To stop the Symantec Data Loss Prevention services on a Linux Enforce Server

1. On the computer that hosts the Enforce Server, log on as root.
2. Stop all running Symantec Data Loss Prevention services by running the following command:

   ```
   service SymantecDLPIncidentPersister stop
   service SymantecDLPManager stop
   service SymantecDLPDetectionServerController stop
   service SymantecDLPNotifier stop
   ```

See “Starting an Enforce Server on Linux” on page 75.

Starting a detection server on Linux

Use the following procedure to start the Symantec Data Loss Prevention services on a Linux detection server.

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

1. On the computer that hosts the detection server, log on as root.
2. Start the Symantec Data Loss Prevention service by running the following command:

   ```
   service SymantecDLPDetectionServer start
   ```

See “Stopping a detection server on Linux” on page 76.

Stopping a detection server on Linux

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

To stop the Symantec Data Loss Prevention services on a Linux detection server

1. On the computer that hosts the detection server, log on as root.
2. Stop the Symantec Data Loss Prevention service by running the following command:

   ```
   service SymantecDLPDetectionServer stop
   ```

See “Starting a detection server on Linux” on page 76.
Starting services on single-tier Linux installations

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

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

1. On the computer that hosts the Symantec Data Loss Prevention server applications, log on as root.

2. Start the Symantec DLP Notifier service by running the following command:

   service SymantecDLPNotifier start

3. Start the remaining Symantec Data Loss Prevention services by running the following command:

   service SymantecDLPManager start
   service SymantecDLPDetectionServer start
   service SymantecDLPIncidentPersister start
   service SymantecDLPDetectionServerController start

See “Stopping services on single-tier Linux installations” on page 77.

Stopping services on single-tier Linux installations

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

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

1. On the computer that hosts the Symantec Data Loss Prevention servers, log on as root.

2. Stop all running Symantec Data Loss Prevention services by running the following command:

   service SymantecDLPIncidentPersister stop
   service SymantecDLPManager stop
   service SymantecDLPDetectionServer stop
   service SymantecDLPDetectionServerController stop
   service SymantecDLPNotifier stop

See “Starting services on single-tier Linux installations” on page 77.
Symantec Data Loss Prevention upgrade troubleshooting and recovery

This chapter includes the following topics:

- About troubleshooting Symantec Data Loss Prevention upgrade problems
- Troubleshooting Enforce Server services
- Rolling back to the previous Symantec Data Loss Prevention release
- Creating the Enforce Reinstallation Resources file
- Uninstalling a server from a Linux system

About troubleshooting Symantec Data Loss Prevention upgrade problems

If you experience problems with completing a successful product upgrade, see these topics:

- See “Troubleshooting Enforce Server services” on page 79.
- See “Rolling back to the previous Symantec Data Loss Prevention release” on page 79.
Troubleshooting Enforce Server services

If the Symantec Data Loss Prevention services do not start after you upgrade your system, check the log files for possible issues (for example, connectivity, password, or database access issues).

- The Symantec Data Loss Prevention installation log is

- Symantec Data Loss Prevention operational logs are in
  /var/log/Symantec/DataLossPrevention/<Enforce Server> or <Detection Server>/15.1/directory.

- Oracle logs can be found in
  $ORACLE_BASE/diag/rdbms/protect/protect/trace/alert_protect.log
  on the Oracle server computer.

Rolling back to the previous Symantec Data Loss Prevention release

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

To roll back to a previous release, you must have the following available:

- 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.

See "Reverting the Enforce Server to a previous release" on page 80.

See "Reverting a detection server to the previous release" on page 80.
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).

Note: This procedure assumes that you have not uninstalled the previous Symantec Data Loss Prevention version Enforce Server and detection servers.

To revert an Enforce Server upgrade to the previous release

1. Stop all Symantec Data Loss Prevention services that are running on the version 15.1 Enforce Server.
   See “About Symantec Data Loss Prevention services” on page 73.

2. Disable all Symantec Data Loss Prevention services that are running on the version 15.1 Enforce Server.

3. Stop all the Oracle services.

4. Restore the Symantec Data Loss Prevention Oracle database from the latest backup.
   Consult your Oracle documentation for more information.
   The restored database files should be owned by the oracle user. If they are not, set the owner on the /opt/oracle/oradata/protect directory (this directory is the default directory for Oracle installation; your deployment may use different directory) by running the following command as the root user:
   
   ```bash
   chown -R oracle:oinstall protect
   ```

5. Restart all the Oracle services.
   Consult your Oracle documentation for more information.

6. Enable the services on the previous Symantec Data Loss Prevention version.

7. Start services on the previous Symantec Data Loss Prevention version.

Reverting a detection server to the previous release

Perform the detection server rollback after you complete the Enforce Server rollback. If you roll back the detection server first, the detection server displays a Unknown status on the System > Servers and Detectors > Overview > Server / Detector Detail screen.

See “Reverting the Enforce Server to a previous release” on page 80.

See "Rolling back to the previous Symantec Data Loss Prevention release" on page 79.
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.
   
   See “About Symantec Data Loss Prevention services” on page 73.

2. Enable the services on the previous Symantec Data Loss Prevention version.

3. Start services on the previous Symantec Data Loss Prevention version.

Creating the Enforce Reinstallation Resources file

Before you uninstall Symantec Data Loss Prevention, create an EnforceReinstallationResources.zip file using the Reinstallation Resources Utility. This file includes the CryptoMasterKey.properties file and the keystore files for your Symantec Data Loss Prevention deployment.

Each Symantec Data Loss Prevention installation encrypts its database using a unique CryptoMasterKey.properties file. An exact copy of this file is required if you intend to reuse the existing Symantec Data Loss Prevention database. If the CryptoMasterKey.properties file becomes lost or corrupted and you do not have a backup, contact Symantec Technical Support to recover the file.

Follow this procedure to create the EnforceReinstallationResources.zip file required by the Symantec Data Loss Prevention 15.1 installer.

To create the Enforce Reinstallation Resources file

1. Locate the ReinstallationResourcesUtility.sh at /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/bin.

2. Generate an Enforce Reinstallation Resources file by running the following command:

   ./ReinstallationResourcesUtility.sh export \Enforce Server\15.1\Protect \opt\EnforceReinstallationResources.zip

3. Use this new EnforceReinstallationResources.zip when reinstalling Symantec Data Loss Prevention from your backup version.
Uninstalling a server from a Linux system

To uninstall a Linux server

1 Before running the uninstaller, back up all keystore files in the
   /opt/Symantec/DataLossPrevention/Enforce Server/15.1/protect/keystore
directory by creating an Enforce Reinstallation Resources file.

   See “Creating the Enforce Reinstallation Resources file” on page 81.

---

Note: The uninstallation process deletes all files and directories created by the installer.
2 Run an uninstallation command to remove a server or component.

**JRE**

```
rpm -e
symantec-dlp-server-jre-1-8-0-162-1.8.0.162-1.el6.x86_64
```

**Enforce Server**

```
rpm -e
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64
symantec-dlp-enforce-server-system-dependencies-1.0.0-1.el6.x86_64
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x84_64
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x84_64
```

**Detection server**

```
rpm -e
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x84_64
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x84_64
```

**Remote indexer**

```
rpm -e
symantec-dlp-15-1-indexers-15.1-1.el6.x86_64
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64
```

**Single-tier installation**

```
rpm -e
symantec-dlp-15-1-single-tier-server-15.1-1.el6.x86_64
symantec-dlp-15-1-enforce-server-15.1-1.el6.x86_64
symantec-dlp-15-1-detection-server-15.1-1.el6.x86_64
symantec-dlp-15-1-server-platform-common-15.1-1.el6.x86_64
symantec-dlp-enforce-server-system-dependencies-1.0.0-1.el6.x86_64
symantec-dlp-keyview-11-4-11.4.0.0-1.el6.x86_64
symantec-dlp-15-1-content-extraction-plugins-15.1-1.el6.x84_64
symantec-dlp-15-1-content-extraction-service-15.1-1.el6.x84_64
```

---

**Note:** You can run the following command to remove all RPMs that start with "symantec":

```
rpm -e $(rpm -qa "symantec")
```
Index

A
Agent configuration
   updating 43
Agent upgrade 17, 26, 44, 53–54

B
Backward compatibility
   Symantec DLP Agents and servers 17

D
detection servers
   requirements 16
   reverting to the previous release 80
disk space 16
DLPDownloadHome directory 26

E
Endpoint Prevent group directories
   upgrading 43
Enforce Server
   requirements 16
Enforce server installation
   installation steps 29

G
group directories
   upgrading 43

I
installation
   uninstalling 82

K
known issues 21

L
language packs
   upgrading 21
   languages
      language packs 21

O
Oracle database
   preparations 10
oracle_create_user.sql script 13

P
post-upgrade tasks 63
   verifying 63
preparations
   detection servers 42
   Oracle database 10
   software download 26

R
requirements
   Enforce Server 16
   reverting upgrade
      detection servers 80

S
scanners 43
single-tier installation
   ProtectInstaller64_15.1.exe 38
SingleTierServer.zip 38
software download 26
SQL scripts 13
Symantec DLP Agent
   backward compatibility for agents and servers 17
   installing with system management software 60
   Mac
      installed aspects 61
      upgrade 56
   upgrading major versions manually 53
   upgrading major versions silently 54
   upgradingversions 44
Symantec DLP services
   starting 75–77
Symantec DLP services  (continued)
  stopping 75–77

U
uninstalling 82
upgrade 63
  See also post-upgrade tasks
detection servers 42
disk space 16
known issues 21
Oracle database 10
phases 9
requirements 16
scanners 43
software download 26
stages 9
verifying 63

upgrading
  major versions 44

V
verifying the upgrade 63