Symantec™
A Division of Broadcom

Symantec Data Loss Prevention Upgrade Guide for Linux

Version 15.7

Last updated: September 15, 2021

Table of Contents

Preparing to upgrade 5
About updates to the Symantec Data Loss Prevention Upgrade Guide 5
About preparing to upgrade Symantec Data Loss Prevention 5
Symantec Data Loss Prevention upgrade phases 6
Preparing the Oracle database for a Symantec Data Loss Prevention upgrade 7
Checking the database update readiness 7
Preparing to run the Update Readiness Tool 8
Creating the Update Readiness Tool database account 12
Running the Update Readiness Tool from the Enforce Server administration console 14
Running the Update Readiness Tool at the command line 14
Reviewing update readiness results 15
Switching from SID to SERVICE_NAME 17
Switch from SID to SERVICE_NAME 17
Register the service name 18
Setting ORACLE_HOME and PATH variables 18
Set the ORACLE_HOME and path variable on Linux 18
Confirming the Oracle database user permissions 18
About the minimum system requirements for upgrading to the current release 19
Supported upgrade backward compatibility for agents and servers 19
About the requirement for language pack upgrades 20
Upgrade requirements and restrictions 20
Preparing your system for the upgrade 21
About external storage for incident attachments 21
Upgrading to a new release 23
Upgrading Symantec Data Loss Prevention 23
Downloading and extracting the upgrade software 24
Signing RPM files 24
Migrating the previous version to a new Enforce Server installation 25
Installing the Java Runtime Environment on the Enforce Server 26
Installing an Enforce Server 26
Update the Schema_Objects_Validation_b.sql file if running Oracle 19c 27
Running the Migration Utility on the Enforce Server 27
Migrate silently 27
Migrate using interactive mode 28
Migrating a previous version detection server to the latest version 28
Installing the Java Runtime Environment on a detection server 29

Installing a detection server 29
Running the Migration Utility on a detection server 30
Migrate using silent mode 30
Migrating previous version data to a new single-tier installation 31
Installing the Java Runtime Environment for a single-tier installation 31
Installing a single-tier server 32
Running the Migration Utility on single-tier installation 32
Migrate using silent mode 33
Migrate using interactive mode 33
Parameters for install.sh 33
Verifying that the Enforce Server and the detection servers are running 34
Applying the updated configuration to Endpoint Prevent servers 35
Upgrading your scanners 35
Upgrading Endpoint Prevent group directory connections 35
Updating an appliance 35
Upgrading Symantec DLP Agents 36
About Symantec Data Loss Prevention Agent upgrades 36
About secure communications between DLP Agents and Endpoint Servers 37
Generating agent installation packages 37
Agent installation package contents 40
Working with endpoint certificates 41
Process to upgrade the DLP Agent on Windows 41
Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled 42
Upgrading the Windows agent manually 42
Upgrading the Windows agent silently 42
Process to upgrade the DLP Agent on Mac 43
Packaging Mac agent upgrade files 44
Upgrading the DLP Agent for Mac manually 45
Upgrading DLP Agents on Mac endpoints silently 46
Confirming that the Mac agent is running 46
What gets upgraded for DLP Agents on Mac endpoints 46
Post-upgrade tasks 48
Performing post-upgrade tasks 48
Verifying Symantec Data Loss Prevention operations 48
Migrating plug-ins 49
About securing communications between the Enforce Server and the database 49
About orapki command line options 49
Using orapki to generate the server certificate on the Oracle database 50
Configuring communication on the Enforce Server 51

Configuring the server certificate on the Enforce Server.......... 53

Verifying the Enforce Server database certificate usage.......... 53

About remote indexers.......... 54

About updating the JRE to the latest version.......... 54

Steps to update the JRE.......... 54

Installing the OpenJRE.......... 54

Updating the JRE to the latest version on Linux.......... 55

Update the JRE using interactive mode.......... 55

Update the JRE using silent mode.......... 55

Reverting a JRE version to a previous release.......... 56

Reverting the JRE on Linux.......... 56

Starting and stopping services.......... 57

About Symantec Data Loss Prevention services.......... 57

Increase the Max Memory.......... 57

About starting and stopping services on Linux.......... 58

Starting an Enforce Server on Linux.......... 58

Stopping an Enforce Server on Linux.......... 58

Starting a detection server on Linux.......... 58

Stopping a detection server on Linux.......... 59

Starting services on single-tier Linux installations.......... 59

Stopping services on single-tier Linux installations.......... 59

Symantec Data Loss Prevention upgrade troubleshooting and recovery.......... 60

About troubleshooting Symantec Data Loss Prevention upgrade problems.......... 60

Troubleshooting Enforce Server services.......... 60

Rolling back to the previous Symantec Data Loss Prevention release.......... 60

Reverting the Enforce Server to a previous release.......... 61

Reverting a detection server to the previous release.......... 62

Creating the Enforce Reinstallation Resources file.......... 62

Creating the Enforce Reinstallation Resources file on Linux.......... 63

Uninstalling a server from a Linux system.......... 63

Applying a Maintenance Pack.......... 64

Steps to apply a maintenance pack on Linux servers.......... 64

Downloading and extracting the maintenance pack software for Linux servers.......... 64

Updating the Enforce Server on Linux.......... 64

Updating the detection server on Linux.......... 65

Updating a single-tier system on Linux.......... 65

Copyright statement.......... 67

Preparing to upgrade

Learn about preparing to upgrade the Enforce Server and detection servers on Linux.

About preparing to upgrade Symantec Data Loss Prevention

Symantec Data Loss Prevention upgrade phases

About the minimum system requirements for upgrading to the current release

About the requirement for language pack upgrades

Preparing the Oracle database for a Symantec Data Loss Prevention upgrade

Supported upgrade backward compatibility for agents and servers

Upgrade requirements and restrictions

Preparing your system for the upgrade

About updates to the Symantec Data Loss Prevention Upgrade Guide

This guide is occasionally updated as new information becomes available.

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

Table 1: Change history for the Symantec Data Loss Prevention Upgrade Guide for Linux

Date	Change description
15 September 2021	Corrected steps for running the Reinstallation Resources Utility. Clarified server uninstallation instructions to only remove DLP components.
4 March 2021	Added steps for installing OpenJRE. Clarified that custom scripts and custom plugins are not moved to the new instance during the migration process. Corrected the location where the Symatec-provided JRE installation files are located.
22 September 2020	Indicated that `/tmp/MacInstaller` is the required location from where the create_package should be run on macOS 10.15.x and later. Removed requirement to convert database to SecureFiles format.
31 July 2020	Added steps for applying the latest `Schema_Objects_Validation_b.sql` file. Applying the latest file is required for users running the Oracle 19c database who plan to upgrade to Symantec Data Loss Prevention version 15.7.
2 June 2020	Added steps for using the install.sh command to apply Maintenance Packs. Added updates to the Update Readiness Tool process.

About preparing to upgrade Symantec Data Loss Prevention

To review the new features for Symantec Data Loss Prevention 15.7, see the *What's New and What's Changed in Symantec Data Loss Prevention 15.7*: Related Documents.

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 15.7 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 15.7, 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 15.7 detection servers.

Upgrade requirements and restrictions

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 (available at Related Documents).

Symantec Data Loss Prevention upgrade phases

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

Table 2: Symantec Data Loss Prevention upgrade phases

Phase	Action	Description
1	Review important information about the new release before starting the upgrade, including: • Known release issues. • Minimum system requirements. • Language pack requirements. • *What's New and What's Changed*.	See the *Symantec Data Loss Prevention 15.7 Release Notes* at Related Documents 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 Related Documents for information about new and changed features in Symantec Data Loss Prevention . About the minimum system requirements for upgrading to the current release About the requirement for language pack upgrades
2	Prepare the system for upgrading. This preparation includes the following items: • Back up the Oracle database and detection server data. If the upgrade fails you can use these backups to restore your system. • Prepare the Update Readiness Tool. • Create the Enforce Reinstallation Resources file.	Preparing your system for the upgrade
3	Download and extract the version 15.7 software.	Downloading and extracting the upgrade software
4	Upgrade the Enforce Server, which includes the following steps: • Install the Java Runtime Environment. • Install the version 15.7 Enforce Server. • Run the Update Readiness Tool. If you find issues, fix them before you migrate your data to version 15.7. • Update the `Schema_Objects_Validation_b.sql` file (if running Oracle 19c). • Migrate the previous version to the version 15.7 Enforce Server.	Migrating previous version data to a new Enforce Server installation Migrating previous version data to a new single-tier installation

Phase	Action	Description
5	Upgrade detection servers, which includes the following steps: • Install the Java Runtime Environment. • Install the version 15.7 detection server. • Migrate the previous version to the version 15.7 detection server.	Migrating a previous version detection server to the latest version
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 15.7 detection servers.	Implementing Symantec DLP Agent Endpoint management
7	Upgrade any scanners.	Upgrading your scanners
8	Complete the required and optional post-upgrade tasks.	Performing post-upgrade tasks

Preparing the Oracle database for a Symantec Data Loss Prevention upgrade

The following Oracle-related preparations must be made before you upgrade the Symantec Data Loss Prevention database schema for version 15.7:

Table 3: Preparing the Oracle database for upgrade

Step	Action	Description
1	Back up the Oracle database before you start the upgrade. You cannot recover from an unsuccessful upgrade without a backup of your Oracle database.	See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* at Related Documents.
2	Run the Update Readiness Tool to confirm that the Oracle database is ready to upgrade to Symantec Data Loss Prevention version 15.7.	Checking the database update readiness
3	Switch the Oracle `SID` to `SERVICE_NAME` if you are upgrading from Symantec Data Loss Prevention version 14.x through 15.1.x. These versions use the Oracle `SID`. You cannot complete the upgrade process if you do not switch to the `SERVICE_NAME` parameter. **Note:** If you are running a fresh installation of version 15.1 that was downloaded on or after 21 September 2018, you can skip this step. This version uses the `SERVICE_NAME` by default.	Switching from SID to SERVICE_NAME
4	Set ORACLE_HOME and PATH variables.	Setting ORACLE_HOME and PATH variables
5	Confirm that the database user has permissions to connect to the Enforce Server.	Confirming the Oracle database user permissions
6	On single- and two-tier installations, add SQL*Plus to the protect user's path.	Add SQL*Plus to the protect user path

Preparing your system for the upgrade

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.

NOTE
You can run the Update Readiness Tool while Symantec Data Loss Prevention continues to run.

Symantec recommends that you prepare for the upgrade, including running the Update Readiness Tool, a few weeks before you plan to complete the upgrade process. Preparing helps ensure that any issues that arise can be resolved before the scheduled completion date.

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

Using the Update Readiness Tool lists tasks you complete to run the tool.

Table 4: Using the Update Readiness Tool

Step	Task	Details
1	Prepare to run the Update Readiness Tool.	Preparing to run the Update Readiness Tool
2	Create the Update Readiness Tool database account.	Creating the Update Readiness Tool database account
3	Run the tool.	You can run the tool for the following scenarios: • From the Enforce Server. Running the Update Readiness Tool at the command line • From the command line on the Enforce Server host computer. Running the Update Readiness Tool from the Enforce Server administration console • For Amazon RDS for Oracle. See the "Preparing the Amazon RDS for Oracle for upgrade" topic in the Symantec Data Loss Prevention Help for information.
4	Review the update readiness results.	Reviewing update readiness results

Preparing to run the Update Readiness Tool

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

1. Obtain the current version of the tool from Product Downloads at the Broadcom Support Portal.

   The current version of the Update Readiness Tool includes important fixes and improvements, and should be the version that you use before attempting any upgrade.

   Symantec recommends that you download the tool to the directory `DLPDownloadHome/DLP/15.7/`.

NOTE

Review the Readme file that is included with the tool for a list of Symantec Data Loss Prevention versions the tool can test.

2. (Optional) Confirm that you have converted the LOB tables from BasicFiles to SecureFiles format.

   About converting LOB tables from BasicFiles to SecureFiles format
3. Log on as Administrator to the database server system.
4. Confirm the following prerequisites if you are running a three-tier deployment:
   - You are running the same Oracle Client version as the Oracle Server version.

     If the versions do not match, the Oracle Client cannot connect to the database, which causes the Update Readiness Tool to fail.
   - The Oracle Client is installed as Administrator.

     If the Oracle Client is not installed as Administrator, reinstall it and select **Administrator** on the **Select Installation Type** panel. Selecting **Administrator** enables the command-line clients, `expdp` and `impdp`.
5. Shut down all but one instance of the database on RAC nodes if you are upgrading on a system that uses Oracle RAC.
6. Stop Oracle database jobs if your database has scheduled jobs.

   Stopping Oracle database jobs
7. Unzip the `Update_Readiness_Tool.zip` file, and then copy the contents of the unzipped folder to the following location. The contents of the tool folder must reside directly in the `URT` folder as specified:
   - `opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/Migrator/URT/`

   During the upgrade process, the Migration Utility runs the Update Readiness Tool from this location.

Related Links

Checking the database update readiness on page 7

Running the Update Readiness Tool from the Enforce Server administration console on page 14

Running the Update Readiness Tool at the command line on page 14

About converting LOB tables from BasicFiles to SecureFiles format

If you are preparing to upgrade Symantec Data Loss Prevention, Symantec strongly recommends that you convert LOB tables from BasicFiles to SecureFiles format. Symantec recommends converting to SecureFiles format to optimize Symantec Data Loss Prevention database performance. Using SecureFiles format allows the database to reclaim storage and improves query performance. SecureFiles format also allows you to manage your LOB tablespaces.

You use the Symantec Data Loss Prevention database space reclamation utility (`DLP_Lobspace_reclaim.sql`) to convert the database to SecureFiles format. You can perform the conversion before upgrading to the latest version of Symantec Data Loss Prevention. You can convert the database after the upgrade using online redefinition.

Unlike BasicFiles LOB storage, SecureFiles LOB storage is sized as needed for LOB data. This allows the Oracle database to track when the data is deleted and make that space available for new LOB data (within the same LOB segment) after the retention period has expired. While allocated space to the segment does not return to the tablespace, it does not grow if the data being created within that segment is less than or equal to the data being deleted within the same segment as incidents are deleted. Using SecureFiles LOB storage eliminates the need to run the space reclamation script.

If you are upgrading to Oracle 12c, convert your Oracle 11g BasicFiles LOB storage tables to SecureFiles LOB storage format before running the Upgrade Readiness Tool and upgrading. Refer to Convert Oracle 11g BasicFiles LOB storage tables to SecureFiles LOB storage format for Oracle 12c Enterprise for steps to complete.

If you run the `DLP_Lobspace_reclaim.sql` on Symantec Data Loss Prevention 14.6 or 15.x, and you are using Oracle 12c R2 Standard Edition (12.2.0.1), the script fails with this message: "ERROR at line 1: ORA-00439: feature not enabled: Online Redefinition." You can refer to `lobspace_reclamation.log` for error information. Refer to Manually convert Oracle 12c LOB tables from BasicFiles to SecureFiles for steps to complete the conversion.

Oracle 12c Standard Edition does not support online table redefinition, which is used by the Symantec database space reclamation utility.

> **NOTE**
> Previously released versions of the utility only worked for Oracle 11g Standard databases which allowed the use of the online table redefinition.

Convert Oracle 11g BasicFiles LOB storage tables to SecureFiles LOB storage format for Oracle 12c Enterprise

Complete the following steps if you are upgrading to Oracle 12c Enterprise. Convert your Oracle 11g BasicFiles LOB storage tables to SecureFiles LOB storage format before running the Upgrade Readiness Tool and upgrading.

This solution applies to Oracle 11g Standard (11.2.0.4), Oracle 11g Enterprise (11.2.0.4), Oracle 12c Enterprise (12.1.x and 12.2.x), and Oracle 19c Enterprise (19.x) databases and allows you to continue running your system during the conversion process.

> **NOTE**
>
> This solution cannot be applied to Oracle 12c Standard (or later) databases. See Manually convert Oracle 12c LOB tables from BasicFiles to SecureFiles if you are on Oracle 12c or 19c Standard.

Symantec provides an update to the LOB space management script (`DLP_lobspace_mgmt_b.pls`). The updated script converts BasicFiles Large Object (LOB) storage to SecureFiles LOB storage in your database when you run the database space reclamation utility (`DLP_Lobspace_reclaim.sql`).

Unlike BasicFiles LOB storage, SecureFiles LOB storage tracks deleted LOBs and makes that space available after the retention period expires. After converting to SecureFiles LOB storage, you do not need to run a script to reclaim LOB space in your database. Space reclamation is handled automatically.

Complete the following steps to convert BasicFiles LOB storage tables to SecureFiles LOB storage format:

1. Update the LOB space management script.

   Update the LOB space management script

2. Convert the Oracle 11g or Oracle 12c Enterprise database to SecureFiles LOB storage.

   Convert the Oracle 11g or Oracle 12c Enterprise database to SecureFiles LOB storage

Update the LOB space management script
Updating the LOB space management script requires that you update the `DLP_lobspace_mgmt_b.pls` and `DLP_Lobspace_reclaim.sql` files.

The process to update your database to use SecureFiles for LOB storage requires roughly the same amount of space that the LOB_tablespace currently takes up. For example, if your LOB_tablespace takes up 20 GB, you need an extra 20 GB of space in LOB_tablespace to successfully complete the update. After you complete the process, the space utilization decreases in the LOB_tablespace, but the database displaces roughly the same amount of disc space that is required to complete the update.

> **NOTE**
> If your server does not have the disc space that is required to convert the database to SecureFiles using the `DLP_Lobspace_reclaim.sql` script, you can manually convert the LOB_tablespace. SeeManually convert Oracle 12c LOB tables from BasicFiles to SecureFiles.

If the database uses only one data file, add more to accommodate the space that is required to run online redefinition. See article TECH159990.

> **NOTE**
>
> You cannot delete data files later. However, the size of the added data files eventually shrinks.

Incidents continue to be written to the Enforce Server during the SecureFile format conversion process. The process does not affect Enforce Server functions and there is minimal performance impact.

To update the files on Symantec Data Loss Prevention systems, follow these steps:

1. Obtain the latest LOB space management script by completing the following steps:
   a) Download `LOB_Space_Management_Script-September2019.zip` available at the article TECH252716.
   b) Move the file to a temporary location on your Enforce Server computer.
2. Navigate to where the `DLP_lobspace_mgmt_b.pls` and `dlp_lobspace_reclaim.sql` files are located on the Enforce Server (replace vv.u with the Symantec Data Loss Prevention version):
   - `/opt/Symantec/DataLossPrevention/Enforce Server/vv.u/Protect/install/sql`
3. Rename the `DLP_lobspace_mgmt_b.pls` and `DLP_Lobspace_reclaim.sql` files.
4. Extract the new `DLP_lobspace_mgmt_b.pls` and `DLP_Lobspace_reclaim.sql` files from the **LOB_Space_Management_Script-September2019.zip** file to the same directory.

Convert the Oracle 11g or Oracle 12c Enterprise database to SecureFiles LOB storage
Before you convert the database to SecureFiles LOB storage, you update the LOB space management script.
Update the LOB space management script

To use the database space reclamation utility to convert your Oracle 11g BasicFiles LOB storage to SecureFiles LOB storage, complete the following procedure:

1. Perform a cold backup of Oracle database before making any changes.

   See the *Symantec Data Loss Prevention System Maintenance Guide* for steps to perform a cold backup of the Oracle database. This guide is available at the Tech Docs Portal.
2. Open a command prompt and navigate to the directory that contains the database space reclamation script. Refer to step 2 in Update the LOB space management script for the location.
3. Connect to sqlplus as the SYS user:

   ```
   sqlplus sys/<password> as sysdba
   ```
4. Run the database space reclamation utility:

   ```
   @DLP_Lobspace_reclaim.sql
   ```
5. Run the following query to verify that the tables are in SecureFiles LOB storage format:

   ```
   select table_name, securefile from user_lobs where table_name like '%LOB%';
   ```

   The query returns *yes* in the `securefile` column to indicate that the tables are in SecureFiles LOB storage format.

Manually convert Oracle 12c LOB tables from BasicFiles to SecureFiles

This solution applies to all supported databases and requires that you shut down the system during the conversion process.

Unlike BasicFiles LOB storage, SecureFiles LOB storage tracks deleted LOBs and makes that space available after the retention period expires. After converting to SecureFiles LOB storage, you do not need to run a script to reclaim LOB space in your database. Space reclamation is handled automatically.

If you are using an Oracle 12c Standard database that still includes BasicFiles LOB storage tables, you should convert them as soon as possible. Converting takes advantage of the improved functionality of the SecureFiles LOB storage format. You must convert your tables to SecureFiles format before running the Upgrade Readiness Tool when upgrading to the next release of Symantec Data Loss Prevention.

You can manually convert your Oracle 12c LOB tables from BasicFiles to SecureFiles using the following procedure:

1. Perform a cold backup of Oracle database before making any changes.

   See the *Symantec Data Loss Prevention System Maintenance Guide* for steps to perform a cold backup of the Oracle database. This guide is available at the Tech Docs Portal.

2. Shut down all DLP services on your Enforce Server.

Stopping Oracle database jobs

If your database has scheduled jobs, you must unschedule them and clear the jobs queue before you run the Update Readiness Tool and start the migration process. After the jobs are unscheduled and the jobs queue is clear, you can run the Update Readiness Tool and continue your migration.

1. Log on to SQL*Plus using the Symantec Data Loss Prevention database user name and password.
2. Run the following:

   ```
   BEGIN
       FOR  rec IN (SELECT * FROM user_jobs)  LOOP
           dbms_job.broken( rec.job, true);
           dbms_job.remove( rec.job);
       END LOOP;
                 END;
   ```

3. Verify that all jobs are unscheduled by running the following:

   ```
   select count(*) from user_jobs;
   ```

   Confirm that the count is zero. If the count is not zero, run the command to clear the queue again. If a job is running when you attempt to clear the queue, the job continues to run until it completes and is not cleared. For long running jobs, Symantec recommends that you wait for the job to complete instead of terminating the job.

4. Exit SQL*Plus.

Creating the Update Readiness Tool database account

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

1. Navigate to the `/script` folder where you extracted the Update Readiness Tool.
2. Start SQL*Plus:

   ```
   sqlplus /nolog
   ```

3. Run the `oracle_create_user.sql` script:

   ```
   @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 Service Name** prompt, enter a service name for the Oracle Service 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.

   Run the following command if you are running the Oracle database in a non-RAC environment:

   ```
   sqlplus sys/<password> 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];
   ```

9. Run the following command if you are running the Oracle database in a RAC environment:

   ```
   sqlplus sys/<password>@<RAC node ip>:1521/protect as sysdba
   GRANT READ,WRITE ON directory DATA_PUMP_DIR TO [schema user name];
   ```

10. Confirm that the password for the new upgrade readiness database account is compatible with the `expdp` and `impdp` commands by running the following command:

    ```
    expdp <oracle_username>/<password>@<oracle_service_name> dumpfile=sandbox.dmp schemas=<oracle_username>
     content=metadata_only directory=<dpdir> logfile=exp_sandbox.log reuse_dumpfiles=y exclude=grant
    ```

    If the command returns password errors, create a password that meets both Oracle password and EXPDP/IMPDP password requirements (expdp/impdp are OS commands).

Table 5: Parameters for the expdp and impdp compatibility command

Parameter	Value
<oracle_username>	The Symantec Data Loss Prevention database user name.
<password>	The Symantec Data Loss Prevention database password.
<oracle_service_name>	The database service name (typically “protect”).
<dpdir>	The `DATA_PUMP_DIR` location. You use this parameter if you have opted to use a custom data pump directory location.

Related Links

Preparing to run the Update Readiness Tool on page 8
Checking the database update readiness on page 7

Running the Update Readiness Tool from the Enforce Server administration console

You can run the Update Readiness Tool from the Enforce Server administration console to check the update readiness for the next Symantec Data Loss Prevention version. To run the tool, you must have User Administration (Superuser) or Server Administration user privileges.

1. Go to **System > Servers and Detectors > Overview**, and click **System Servers and Detectors Overview**.
2. Click **Upload the Update Readiness Tool** and locate the tool.

   If you the tool has already been uploaded, and you upload a new version, the old version is deleted.

   Preparing to run the Update Readiness Tool
3. Enter the Update Readiness Tool database account user credentials.

   WARNING

   Do not enter the Oracle database user (typically "protect") credentials. Entering credentials other than the Update Readiness Tool database account overwrites the Symantec Data Loss Prevention database.
4. Click **Run Update Readiness Tool** to begin the update readiness check.

   You can click **Refresh this page** to update the status of the readiness check. When you refresh, a link to a summary of results returned at that point in time displays. The process may take up to an hour depending on the size of the database.

   When the tool completes the test, you are provided with a link you can use to download the results log.

Reviewing update readiness results

Checking the database update readiness

Running the Update Readiness Tool at the command line

You can run the Update Readiness Tool from the command prompt on the database server host computer.

Disable all instances of the DLP database on all but one RAC node if you are upgrading on a system that uses Oracle RAC. Also, run the tool on the active RAC node. Restore instances once the tool has completed.

NOTE

The steps assume that you have logged on as the root to the computer on which you intend to run the Update Readiness Tool.

1. Open a command prompt window.
2. Go to the `URT` directory:
   - `opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/Migrator/URT`
3. Run the Update Readiness Tool using the following command:

```
"/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/bin/java" UpdateReadinessTool
--username <schema user name>
--password <password>
--readiness_username <readiness_username>
--readiness_password <readiness_password>
--service_name <database_system_id>
```

Table 6: Update Readiness Tool command line parameters identifies the command line parameters:

Table 6: Update Readiness Tool command line parameters

Parameter	Description
`--username`	The Symantec Data Loss Prevention schema user name.
`--password`	The Symantec Data Loss Prevention schema password.
`--readiness_username`	The Update Readiness Tool database account user that you created. Creating the Update Readiness Tool database account
`--readiness_password`	The password for the Update Readiness Tool database account user.
`--service_name`	The database system ID (SERVICE_NAME), typically "protect." If you are running the database on RAC, provide the database system ID as *<RAC node ip>*/protect.
`--data_pump`	The Data Pump directory name. You use this optional parameter if you have opted to use a custom data pump directory location.
`--skip_export`	The optional parameter prevents the Update Readiness Tool from exporting from the Symantec Data Loss Prevention schema during the Update Readiness Tool test. Use this parameter for the following scenarios: • If you have already created an export DMP file. • If you plan to export data manually.
`--skip_import`	The optional parameter prevents the Update Readiness Tool from importing data to the Update Readiness Tool schema schema during the Update Readiness Tool test. Use this parameter if you plan to import the data manually.
`--verbose`	The optional parameter provides additional logging detail if you plan to debug the Update Readiness Tool test results.
`--quick`	The optional parameter only runs the database object check and skips the update readiness test.

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.

Preparing to run the Update Readiness Tool

Reviewing update readiness results

Reviewing update readiness results

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 (URT). 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.

NOTE
Symantec recommends that you contact Support prior to upgrading your system to review the URT results.

Table 7: Update Readiness results

Status	Description
Pass	Items that display under this section are confirmed and ready for update.
Warning	If not fixed, items that display under this section may prevent the database from upgrading properly.

Status	Description
Error	These items prevent the upgrade from completing and must be fixed.

Related Links

Resolving the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter" on page 16

Resolving the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter"

When running the Update Readiness Tool before an upgrade from Symantec Data Loss Prevention 14.6 to the current version, the tool returns results in its log file with the error below.

```
Start: Data Foreign Key Constraint Validation - [date and time] Data violations are detected on your schema,
 please use the below query(s) to retrieve the invalid data.
SELECT DISTINCT protocolFilterId AS "PROTOCOLFILTERID" FROM ENDPOINTPROTOCOLFILTER
WHERE protocolFilterId IS NULL OR protocolFilterId NOT IN (SELECT acv.protocolFilterId FROM
AgentConfigurationVersion acv WHERE acv.protocolFilterId IS NOT NULL);
End : Data Foreign Key Constraint Validation - elapsed 0s - FAILED (1 violation)
```

Complete the following steps to resolve the error "Data Foreign Key Constraint Validation for EndPointProtocolFilter":

1. Run the following command to create a data backup:

   ```
   create table EndpointProtocolFilter_nomatch as
   select * from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId FROM
   AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
   ```

2. Run the following command to confirm the record count:

   ```
   select count(*) from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId
   FROM AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
   ```

3. Note the record count.
4. Run the following command to delete data that causes the upgrade to fail:

   ```
   DELETE FROM EndpointProtocolFilter WHERE protocolFilterId NOT IN (SELECT acv.protocolFilterId FROM
    AgentConfigurationVersion acv WHERE acv.protocolFilterId IS NOT NULL);
   ```

5. Confirm that the number of records deleted matches the record count. See step 3. If the record counts do not match, contact Symantec Support.
6. Run the following command to complete the delete operation:

   ```
   commit;
   ```

7. Run the following command to confirm that the number of records match:

   ```
   select count(*) from EndpointProtocolFilter where protocolFilterId not in (select acv.protocolFilterId
   FROM AgentConfigurationVersion acv where acv.protocolFilterId IS NOT NULL);
   ```

Related Links

Reviewing update readiness results on page 15

Resolving the error "Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13"

Complete the following to resolve the "Start: Index Definition Validation - Invalid Non-Primary Key Indexes INCIDENT_N13" error:

1. Stop all Enforce Server services.
2. Start SQL*Plus.

3. Log on as the protect user.
4. Run the following script:

   ```
   DROP INDEX INCIDENT_N13; CREATE INDEX Incident_n13 ON Incident(messageDate);
   ```

5. Restart all Enforce Server services.
6. Run the Update Readiness Tool again.

Related Links

About Symantec Data Loss Prevention Services

Reviewing update readiness results on page 15

Switching from SID to SERVICE_NAME

If you are upgrading from Symantec Data Loss Prevention 15.1 or earlier, you switch the Oracle `SID` to `SERVICE_NAME` before you upgrade. You cannot complete the migration process if you do not switch to the `SERVICE_NAME` parameter.

To switch from `SID` to `SERVICE_NAME`, you update the `tnsnames.ora` file to point to the `SERVICE_NAME`, and then register the service name change on the database.

After you switch to the `SERVICE_NAME` parameter, you can upgrade. See the *Symantec Data Loss Prevention Upgrade Guide* available at Related Documents.

Switch from SID to SERVICE_NAME

Update the `tnsnames.ora` file to point to the `SERVICE_NAME`.

1. Locate the `tnsnames.ora` file.

   The file is located at `$ORACLE_HOME/network/admin` on Linux.

2. Back up the `tnsnames.ora` file before you update it.
3. On Linux, switch to the Oracle user by running the following command:

   ```
   su - oracle
   ```

4. Stop the listener by running the following command:

   ```
   lsnrctl stop
   ```

   You can skip this step if the database is already stopped.

5. Open the `tnsnames.ora` file.
6. Change `SID` to `SERVICE_NAME` for the protect value, where protect is your current `SID`.

   The **Protect** section should read as follows:

   ```
   PROTECT =
       (DESCRIPTION =
           (ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCP)(HOST = <host name>)(PORT = 1521)))
           (CONNECT_DATA =
           (SERVICE_NAME = protect)
           )
       )
   ```

Register the service name

Register the service name change on the database.

1. Launch SQL Plus by running the following command:

   ```
   sqlplus /nolog
   ```

2. Connect to the database by running the following command:

   ```
   conn sys/protect as sysdba
   ```

3. Set the service name by running the following command:

   ```
    alter system set service_names='protect' scope=both;
   ```

   Where protect is your new `SERVICE_NAME`.

4. Set the registry by running the following command:

   ```
   alter system register;
   ```

5. Verify that the Oracle database user (typically "protect") uses the `SERVICE_NAME` parameter by running the following command:

   ```
   select value from v$parameter where name like '%service_name%';
   ```

   Where service_name is the `SERVICE_NAME` parameter that connects to the Oracle database.

   The `SERVICE_NAME` value protect displays in the command prompt.

Setting ORACLE_HOME and PATH variables

You set the ORACLE_HOME and PATH variables before you begin the upgrade process. If you do not set these variables, you cannot complete the migration process during the Enforce Server upgrade.

Set the ORACLE_HOME and path variable on Linux

1. Log on as a root user.

2. In the terminal, run the following command to set the ORACLE_HOME variable. Confirm your Oracle version and installation path before setting this variable. For example:

   ```
   export ORACLE_HOME=/opt/oracle/product/19.3.0.0/db_1
   ```

3. Run the following command to set the PATH variable:

   ```
   export PATH=$ORACLE_HOME/bin:$PATH
   ```

Confirming the Oracle database user permissions

The Oracle database user (typically “protect”) must have permission to connect to the Enforce Server. The installation fails if the user cannot access the Enforce Server.

1. Start SQL*Plus.

2. Run the following commands:

   ```
   sqlplus sys/protect as sysdba
   GRANT read, write ON directory data_pump_dir TO protect;
   GRANT SELECT ON dba_registry_history TO protect;
   GRANT SELECT ON dba_temp_free_space TO protect;
   GRANT SELECT ON v_$version TO protect;
   GRANT EXECUTE ON dbms_lob TO protect;
   ```

3. If you are running Oracle 19c, run the following command:

   ```
   GRANT create job TO protect;
   ```

4. Exit SQL*Plus:

   ```
   exit
   ```

About the minimum system requirements for upgrading to the current release

There are additional package dependencies depending on the version of Linux you are using. See "Third-party software requirements and recommendations" in the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* at Related Documents for detailed information about these additional required packages.

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* at Related Documents.

About preparing to upgrade Symantec Data Loss Prevention

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 15.7, Endpoint Servers on version 15.0, 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 15.7. 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 15.7. 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 15.7.

> **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 15.7 detection servers.

Table 8: Supported backward compatibility for agent upgrades

Enforce Server version	Endpoint Server version	Symantec DLP Agent version	Results
15.7	15.7	15.7	All incidents are sent to the Enforce Server. Policy and configuration updates can be sent to the Endpoint Servers and agents.
15.7	15.7	15.5 15.1 15.0	All incidents are sent to the Enforce Server. Policy and configuration updates can be sent to the Endpoint Servers and agents.
15.7	15.7	14.6 14.5 14.0	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. **Note:** 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 15.7.
15.7	15.5 15.0	14.6 14.5 14.0	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. **Note:** 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.
15.7	14.6 14.5 14.0	14.6 14.5 14.0 12.5.x	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.

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* (available at Related Documents) for information about acquiring and adding updated language packs.

About preparing to upgrade Symantec Data Loss Prevention

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 15.7. You cannot restart Network Discover scans until at least one Network Discover detection server has been upgraded to version 15.7.
- If you have not upgraded a detection server, and it stops (shuts down) after you have upgraded the Enforce Server to version 15.7, you must upgrade that detection server to version 15.7 before it can restart.
- After you upgrade the Enforce Server to version 15.7, any configuration changes that you make have no effect on detection servers not upgraded to 15.7.
- 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 `SymantecDLPDetectionServerControllerService` service to verify the upgraded detection server versions in the Enforce Server administration console.

About preparing to upgrade Symantec Data Loss Prevention

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:

Upgrade requirements and restrictions

Preparing the Oracle database for a Symantec Data Loss Prevention upgrade

Creating the Update Readiness Tool database account

Creating the Enforce Reinstallation Resources file

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

About the minimum system requirements for upgrading to the current release

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 Sever 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 recommends 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 15.7, 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 to a new release

Learn about upgrading the Enforce Server and detection servers on Linux.

Upgrading Symantec Data Loss Prevention

Downloading and extracting the upgrade software

Signing RPM files

Migrating the previous version 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

Parameters for install.sh

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

Updating an appliance

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 that you must perform so that your profiles and policies update properly. See "Updating EDM indexes to the latest version" in the Administration Guide available at Related Documents.

Table 9: Upgrading Symantec Data Loss Prevention

Step	Action	Description
1	Download and extract the upgrade software.	Downloading and extracting the upgrade software
2	Confirm that your existing Enforce Server and detection servers are running.	Verifying that the Enforce Server and the detection servers are running
3	Close all files and folders in your existing Enforce Server environment.	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.
4	Install the Java Runtime Environment on the Enforce Server.	Installing the Java Runtime Environment on the Enforce Server
5	Prepare the Update Readiness Tool.	Preparing to run the Update Readiness Tool
6	Install the version 15.7 Enforce Server.	Installing an Enforce Server

Step	Action	Description
7	Run the Update Readiness Tool on the version 15.7 Enforce Server.	Running the Update Readiness Tool from the Enforce Server administration console
8	Update the `Schema_Objects_Validation_b.sql` file on the version 15.7 Enforce Server.	If you are running Oracle 19c, complete this step. Update the Schema_Objects_Validation_b.sql file if running Oracle 19c
9	Migrate the previous version to the version 15.7 Enforce Server.	Running the Migration Utility on the Enforce Server
10	Install the Java Runtime Environment on the detection server.	Installing the Java Runtime Environment on a detection server
11	Install the version 15.7 detection servers.	Installing a detection server
12	Migrate the previous version to the version 15.7 detection servers.	Running the Migration Utility on a detection server
13	(Optional) Apply the updated agent configuration to Endpoint Prevent detection servers.	Applying the updated configuration to Endpoint Prevent servers
14	(Optional) Update Symantec DLP Agents.	About Symantec Data Loss Prevention Agent upgrades
15	(Optional) Update any scanners.	Upgrading your scanners

Downloading and extracting the upgrade software

1. Download the following ZIP files from Product Downloads at the Broadcom Support Portal:
   - `Symantec_DLP_15.7_Platform_Lin-IN.zip`
   - `Symantec_DLP_15.7_Agent_Win-IN.zip`: (for Endpoint deployments only)
   - `Symantec_DLP_15.7_Agent_Mac-IN.zip` (for Endpoint deployments only)
2. 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.
3. Extract the contents of the `Symantec_DLP_15.7_Platform_Lin-IN.zip` file.
4. Extract the contents of the `Symantec_DLP_15.7_Agent_Win-IN.zip` file.
5. Extract the contents of the `Symantec_DLP_15.7_Agent_Mac-IN.zip` file.
6. Note where you saved the MSI and PKG files so you can quickly find them later.

Symantec Data Loss Prevention upgrade phases

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_15.7_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.

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_15.7_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 the previous version 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.

> **NOTE**
>
> The migration process backs-up services `.conf` files from Symantec Data Loss Prevention 15.5 and later. You can locate these files at `/opt/Symantec/DataLossPrevention/EnforceServer/vv.y/Protect/` in a folder that is formatted as `service-yyyy-mm-dd-hh-mm-ss`. (Replace vv.u with the previous version number.) You use the `.conf` files if you are recovering your previous version system. See the *Symantec Data Loss Prevention System Maintenance Guide* for more information about recovering your system (available at Related Documents).

1. Install the Java Runtime Environment on the Enforce Server.

   Installing the Java Runtime Environment on the Enforce Server

2. Run the Update Readiness Tool.

   Ensure that the database is ready for the migration by running the Update Readiness Tool.

   Preparing to run the Update Readiness Tool

3. Sign RPM files.

   Signing RPM files

4. Install the version 15.7 Enforce Server.

   You install the Enforce Server on the same system where the previous version is running.

   Installing an Enforce Server

5. Migrate the previous version to the version 15.7 Enforce Server.

   Running the Migration Utility on the Enforce Server

The process to migrate does not move all plug-ins. Migrating plug-ins

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.

1. Log on as root to the Enforce Server system on which you intend to install Enforce.
2. Copy `ServerJRE.zip` from your `DLPDownloadHome/DLP/15.7/New_Installs/Release` directory to the computer where you plan to install the Enforce Server.
3. Unzip the file contents (for example, unzip to `/opt/temp`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
4. Install the JRE by running the following command:

   ```
   ./install.sh -t serverjre
   ```

   Parameters for install.sh

Installing an Enforce Server

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

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

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

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
5. Confirm file dependencies for RPM files by running the following command:

   ```
   rpm -qpR *.rpm
   ```

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

   ```
   rpm -qpR .rpm-file
   ```

   If the command indicates that dependancies are missing, you can use YUM repositories to install them. Use the following command:

   ```
   yum install repo
   ```

   Replace repo with the repository package name.
6. Install the Enforce Server by running the following command:

   ```
   ./install.sh -t enforce
   ```

   Parameters for install.sh

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

7. Restart any antivirus, pop-up blocker, or other protection software that you disabled.
8. 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.
9. Start the migration process.

Update the Schema_Objects_Validation_b.sql file if running Oracle 19c

Complete the following procedure if you are running Oracle 19c.

1. Download the ZIP file from Product Downloads at the Broadcom Support Portal: `15_7_Schema_Objects_Validation_b.zip`.
2. Extract `Schema_Objects_Validation_b.sql` from the downloaded zip file.
3. Copy the `Schema_Objects_Validation_b.sql` file to the following location on the Enforce Server:

   ```
   C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.7\Protect\Migrator\SQL
   ```

   ```
   opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/Migrator/SQL
   ```

   > **NOTE**
   > Accept the request to overwrite the existing file.

Running the Migration Utility on the Enforce Server

The Migration Utility moves data, configurations, and custom files (data profiles, plug-ins, and incidents) to the 15.7 instance. The migration utility also stops previous version services and starts new version services.

After you install the version 15.7 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.

You can migrate data silently or using interactive mode.

Migrate silently

Migrate using interactive mode

The process to migrate data does not move all plug-ins. Migrating plug-ins

> **NOTE**
>
> Before you run the Migration Utility, you must switch to `root` user.

Migrate silently

Use the following command to complete the migration silently:

```
./EnforceServerMigrationUtility
-silent
-sourceVersion="<previous version>"
-jreDirectory="/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202"
```

Where <previous version> is the previous version number of the previous active version installation. The path /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202 points to the current JRE location.

Migrate 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/EnforceServer/15.7/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. Confirm the JRE directory that displays.

   If no JRE displays, install the JRE.

   Installing the Java Runtime Environment on the Enforce Server
6. Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.

   NOTE

   If you uninstall the previous version, the service_user is removed.
7. If migration fails, review the Enforce Server migration logs in `MigrationUtility.log` located at `/var/log/Symantec/DataLossPrevention/EnforceServer/15.7/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.

NOTE

The migration process backs up services `.conf` files from Symantec Data Loss Prevention 15.5 and later. You can locate these files at `/opt/Symantec/DataLossPrevention/DetectionServer/vv.u/Protect/` in a folder formatted as `service-yyyy-mm-dd-hh-mm-ss`. (Replace vv.u with the previous version number.) You use the `.conf` files if you are recovering your previous version system. See the *Symantec Data Loss Prevention System Maintenance Guide* for more information about recovering your system.

1. Install the Java Runtime Environment on the detection server.

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

   Installing the Java Runtime Environment on a detection server
2. Sign RPM files.

   Signing RPM files
3. Install the version 15.7 detection servers.

   Installing a detection server
4. Migrate the previous version to the version 15.7 detection servers.

   Running the Migration Utility on a detection server

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.

1. Log on as root to the computer on which you intend to install the detection server.
2. Copy `ServerJRE.zip` from your `DLPDownloadHome/DLP/15.7/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`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
4. Install the JRE by running the following command:

   ```
   ./install.sh -t serverjre
   ```

   Parameters for install.sh

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 `DetectionServer.zip` file has been copied into the `/opt/temp/` directory on the server computer.

1. Complete the preinstallation steps.

   About preparing to upgrade Symantec Data Loss Prevention
2. Log on as root to the computer on which you intend to install the detection server.
3. Copy the detection server installer (`DetectionServer.zip`) from the Enforce Server to a local directory on the detection server. The `DetectionServer.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 `DetectionServer.zip` file (`/opt/temp/`).
5. Unzip the file contents (for example, unzip to `/opt/temp`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
6. Confirm file dependencies for RPM files by running the following command:

   ```
   rpm -qpR *.rpm
   ```

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

   ```
   - rpm -qpR .rpm-file
   ```

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

   If the command indicates that dependancies are missing, you can use YUM repositories to install them. Use the following command:

   ```
   yum install repo
   ```

   Replace repo with the repository package name.

7. Install the detection server by running the following command:

   ```
   ./install.sh -t detection
   ```

   Parameters for install.sh

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

8. Navigate to the migrator directory: `/opt/Symantec/DataLossPrevention/DetectionServer/15.7/Protect/Migrator`

9. Start the migration process.

Running the Migration Utility on a detection server

After you install the version 15.7 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.

Migrate using silent mode

Migrate using interactive mode

NOTE

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

Migrate using silent mode

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

```
./DetectionServerMigrationUtility
-silent
-sourceVersion="<previous version>"
-jreDirectory="/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202"
```

Where <previous version> represents where the previous version number. The /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202 points to the current JRE location.

Migrate 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/DetectionServer/15.7/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. Confirm the JRE directory that displays.

   If no JRE displays, install the JRE.

6. Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.
7. If migration fails, review the detection server migration logs in `MigrationUtility.log` located at `/var/log/Symantec/DataLossPrevention/DetectionServer/15.7/debug/`.

The process to migrate data does not move all plug-ins. Migrating plug-ins

Migrating previous version data to a new single-tier installation

After you install the version 15.7 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.

> **NOTE**
>
> The migration process backs up `.conf` files from Symantec Data Loss Prevention 15.5 and later. You can locate these files at `/opt/Symantec/DataLossPrevention/SingleTierServer/15.7/Protect/` in a folder formatted as `service-yyyy-mm-dd-hh-mm-ss`. (Replace vv.u with the previous version number.) You use the `.conf` files if you are recovering your previous version system. See the *Symantec Data Loss Prevention System Maintenance Guide* for more information about recovering your system (available at Related Documents).

1. Install the Java Runtime Environment on the Enforce Server.

   You can skip this step if you are already running a compatible JRE version.
2. Run the Update Readiness Tool.

   Running the tool identifies potential issues with the database.

   Creating the Update Readiness Tool database account
3. Sign RPM files.

   Signing RPM files
4. Install the version 15.7 single-tier system.

   You install the single-tier system on the same computer where the previous version is running.
5. Migrate the previous version to the version 15.7 single-tier installation.

   Running the Migration Utility on single-tier installation

Installing the Java Runtime Environment for a single-tier installation

You install the Java Runtime Environment (JRE) before you complete a single-tier installation.

1. Log on as root to the computer where you plan to install the single-tier system.
2. Copy `ServerJRE.zip` to the computer where you plan to install the single-tier system.
3. Unzip the file contents (for example, unzip to `/opt/temp`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
4. Install the JRE by running the following command:

   ```
   ./install.sh -t serverjre
   ```

   Parameters for install.sh

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 `SingleTierServer.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.

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 (`SingleTierServer.zip`) from `DLPDownloadHome` to a local directory on the single-tier computer (for example, `/opt/temp/`).
3. Unzip the file contents (for example, unzip to `/opt/temp`).

   If you prompted whether or not to replace `install.sh`, enter `Y` for yes. The `install.sh` is identical for all packages.
4. Confirm file dependencies for RPM files by running the following command:

   ```
   rpm -qpR *.rpm
   ```

   If the command indicates that dependencies are missing, you can use YUM repositories to install them. Use the following command:

   ```
   yum install repo
   ```

   Replace repo with the repository package name.
5. Install the JRE by running the following command:

   ```
   ./install.sh -t singletier
   ```

   Parameters for install.sh

   > **NOTE**
   >
   > If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.
6. Restart any antivirus, pop-up blocker, or other protection software that you disabled.
7. 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.
8. Start the migration process.

Related Links

Configuring a new single-tier installation

Running the Migration Utility on single-tier installation

After you install the version 15.7 single-tier system, you can migrate data using the Migration Utility.

> **NOTE**
> If you are running Oracle 19c, update the `Schema_Objects_Validation_b.sql` before you run the Migration Utility. See Update the Schema_Objects_Validation_b.sql file if running Oracle 19c.

Before you start the migration, use the Upgrade Readiness tool to confirm that the Oracle database is ready for migration. See Checking the database update readiness.

The process to migrate data does not move all plug-ins. Migrating plug-ins

You can use silent mode or interactive mode to complete the migration.

> **NOTE**
>
> Before you run the Migration Utility, you must switch to `root` user.

Migrate using silent mode

Run the following command as root to complete the migration using silent mode:

```
./SingleTierServerMigrationUtility
-silent
-sourceVersion="<previous version>"
-jreDirectory="/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202"
```

Where <previous version> is the previous version number and /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202 points to the current JRE location.

Migrate 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/SingleTierServer/15.7/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. Confirm the JRE directory that displays.

   If no JRE displays, install the JRE.

   Installing the Java Runtime Environment for a single-tier installation
7. If the migration fails, review the single-tier server migration logs on `MigrationUtility.log` located at `/var/log/Symantec/DataLossPrevention/SingleTierServer/15.7/debug/`.

Parameters for install.sh

You can use the following parameters when using install.sh. If you do not change parameters, a default installation is completed.

Table 10: Parameters for install.sh

Parameter	Default	Description
`-t`	N/A	Defines the installation type, which includes the following. Enter one of the following, depending on what you plan to install: • `enforce` • `detection` • `singletier` • `indexers` • `serverjre`
`-i`	`/opt/Symantec/DataLossPrevention`	Defines the path to the installation directory. You can indicate a path where you want to relocate the installation type. **Note:** If you are upgrading from Symantec Data Loss Prevention version 15.5 to version 15.7, do not change the installation directory. The migration fails if a component is installed to a different directory.
`-d`	`/var/Symantec/DataLossPrevention`	Defines the path to the `data` directory.
`-l`	`/var/log/Symantec/DataLossPrevention`	Defines the path to the `logs` directory.
`-r`	`/var/run/Symantec/DataLossPrevention`	Defines the path to the `run` directory.
`-s`	`/var/spool/Symantec/DataLossPrevention`	Defines the path to the `spool` directory.

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 version.

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.

Related Links

Upgrading Symantec Data Loss Prevention on page 23

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.

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 15.7 scanners. To upgrade a scanner, remove the older software and then install the Symantec Data Loss Prevention 15.7 scanner.

For information on adding and removing scanners, see the *Symantec Data Loss Prevention Administration Guide* available at Related Documents.

Symantec Data Loss Prevention upgrade phases

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 available at Related Documents.

Updating an appliance

You update appliance software using the Enforce Server administration console.

For steps to update an appliance, see the *Symantec Data Loss Prevention Administration Guide* available at Related Documents.

Upgrading Symantec DLP Agents

About Symantec Data Loss Prevention Agent upgrades

About secure communications between DLP Agents and Endpoint Servers

Process to upgrade the DLP Agent on Windows

Process to upgrade the DLP Agent on Mac

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 15.7 Endpoint Server. Endpoint Servers are backward-compatible with a DLP Agent for one full release. For example, a version 15.7 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 11: Upgrade process for Symantec DLP Agents

Step	Description	Process
1	Create the Symantec Data Loss Prevention Agent installation package.	You create the agent installation package using the Enforce Server administration console. This package contains a BAT file that you use to upgrade Windows agents and a PKG file you use to upgrade the Mac agents. About secure communications between DLP Agents and Endpoint Servers
2	Bundle the Mac agent installation files if you plan to upgrade Mac agents.	Process to upgrade the DLP Agent on Mac
3	Install the upgrade package on endpoints.	Choose one of the following upgrade methods: • Upgrade the DLP Agent by using silent upgrades. Upgrading the Windows agent silently Upgrading DLP Agents on Mac endpoints silently • Upgrade the DLP Agent manually. Upgrading the Windows agent manually Upgrading the DLP Agent for Mac manually

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.

Related Links

Generating agent installation packages on page 37

Working with endpoint certificates on page 41

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 the DLP Agent.

About secure communications between DLP Agents and Endpoint Servers

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. You generate a single installation package for each endpoint platform where you want to deploy.

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

> **NOTE**
>
> If you plan to install the ICT Clients and ICE Utilities, you use the **System > Agents > Agent Packaging** screen to generate installers. Symantec Data Loss Prevention version 15.7 supports packaging version 15.1 MP2 and 15.5 MP3 ICT Clients and ICE Utilities with the DLP Agent.
>
> See the topic "Generating agent installation packages" in the version 15.5 *Symantec Data Loss Prevention Upgrade Guide* available at Related Documents.

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.
- 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.

Generating the agent installation package provides instructions for generating agent installation packages. The instructions assume that you have deployed an Endpoint Server.

Table 12: Generating the agent installation package

Step	Action	Description
1	Navigate to the **Agent Packaging** page.	Log on to the Enforce Server administration console as an administrator and navigate to the **System > Agents > Agent Packaging** page.
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 15.7 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**. Add the DLP Agent, ICT Client and ICE Utility installer files to a ZIP file. You browse for this ZIP file in the next step.
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**: `AgentInstall-x64_15_7.msi` **Windows 32-bit**: `AgentInstall-x86_15_7.msi` **Mac 64-bit**: `AgentInstall_15_7.pkg`
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.
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. About agent password management
8	Re-enter the Endpoint tools password.	The system validates that the passwords match and displays a message if they do not.

Step	Action	Description
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. The target directory for the Mac agent is set by default.
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. About agent password management
11	Re-enter the uninstall password.	The system validates that the passwords match and displays a message if they do not.
12	(Optional) Select **Install the Symantec ICT Client**.	Select this option to package a version 15.1 or 15.5 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.
13	(Optional) Select **Install the Symantec ICE Utility**.	Select this option to package a version 15.1 or 15.5 ICE Utility with the agent package. **Note:** You must install the ICE Utility before you enable the **Enable Information Centric Encryption** option on the **Agent Configuration > Settings** screen on the Enforce Administration console. **Note:** For more information, see Information Centric Encryption settings for DLP Agents.
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.

Step	Action	Description

15	Save the agent package zip file.	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`
		`AgentInstaller_Mac64.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 3.

16	Install DLP Agents using the agent package.	Once you have generated and downloaded the agent package, you use it to install all agents for that platform.

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.

Generating agent installation packages

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

Table 13: `AgentInstaller_Win32.zip` and `AgentInstaller_Win64.zip` installation package contents

File name	Description
`AgentInstall-x64_15_7.msi` `AgentInstall-x86_15_7.msi`	Windows agent installer
`endoint_cert.pem`	Agent certificate and encryption keys Working with endpoint certificates
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`install_agent.bat`	Use to install the DLP Agent.
`upgrade_agent.bat`	Use to upgrade the DLP Agent.

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

DLP Agent installation overview

Table 14: `AgentInstaller_Mac64.zip` installation package contents

File	Description
`AgentInstall_15_7.pkg`	Mac DLP Agent installer
`AgentInstall.plist`	Mac DLP Agent installation properties configuration file

File	Description
`create_package`	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).
`endoint_cert.pem`	Agent certificate and encryption keys Working with endpoint certificates
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`install_agent.sh`	Use to install the DLP Agent.
`Install_Readme. rtf`	Provides commands for packaging and installing the agent Process to upgrade the DLP Agent on Mac

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.

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.

Related Links

About secure communications between DLP Agents and Endpoint Servers on page 37

Generating agent installation packages on page 37

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. About Symantec Data Loss Prevention Agent upgrades

Table 15: Process to upgrade agents on Windows endpoints

Step	Action	Description
1	Prepare endpoints that have Safe Mode monitoring enabled.	Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled
2	Upgrade the agent. Upgrade an agent manually. You can upgrade an agent manually when you want to test the configuration. Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time.	Upgrading the Windows agent manually Upgrading the Windows agent silently

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 15.7, 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]
```

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.

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.

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="epserver1:8001;epserver2:8001" 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.

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

3. Specify the `msiexec` properties.

For details on entering this information into your particular systems management software, see the software product documentation.

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 by the confirming that the latest version displays in the list.

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. About Symantec Data Loss Prevention Agent upgrades

Table 16: Process to upgrade agents on Mac endpoints

Step	Action	More information
1	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.	Packaging Mac agent upgrade files
2	Upgrade the agent. Upgrade an agent manually. You can upgrade an agent manually when you want to test the configuration. Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time.	Upgrading the DLP Agent for Mac manually Upgrading DLP Agents on Mac endpoints silently
3	Confirm that the Mac agent service is running.	Confirming that the Mac agent is running
4	(Optional) Review the upgraded Mac agent components. These components include the drivers that prevent tampering and keep the agent running.	What gets upgraded for DLP Agents on Mac endpoints

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. About secure communications between DLP Agents and Endpoint Servers

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

   > **NOTE**
   > If you are running macOS 10.15.x and later, unzip the file contents to the `/tmp/MacInstaller` folder. macOS 10.15.x and later prevents the create_package tool from running from default folder locations (for example, `Downloads`, `Documents`, `Applications`, and so on).

   Agent installation package contents

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. About optional installation and maintenance tools

   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 that is named `AgentInstall_WithCertificates.pkg` is created in the location you indicated. Based on the example, `AgentInstall_WithCertificates.pkg` is created at `/tmp/MacInstaller`.

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

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

   Replace com.company.xyz with information specific to your deployment.

About optional installation and maintenance tools

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

The installation and maintenance tools can be found in the `Symantec_DLP_15.7_Agent_Mac-IN.zip` file.

See "About Endpoint tools" in the *Symantec Data Loss Prevention Administration Guide* available at Related Documents.

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

Packaging Mac agent upgrade files

Table 17: Mac agent maintenance tools lists the available tools.

Table 17: Mac agent maintenance tools

Tool type	Description
Maintenance	• vontu_sqlite3 lets you inspect the agent database. • logdump creates agent log files.

Upgrading the DLP Agent for Mac manually

Instructions for installing the DLP Agent on a Mac endpoint 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. Upgrading DLP Agents on Mac endpoints silently

NOTE

The following steps assume that you have generated the agent installation package and completed all prerequisites. About secure communications between DLP Agents and Endpoint Servers

Table 18: Instructions for upgrading the DLP Agent on a Mac endpoint

Step	Action	Description
1	Locate the agent installation package ZIP (`AgentInstaller_Mac64.zip`), and unzip it to the Mac endpoint.	Unzip the file to `/tmp/MacInstaller`. Symantec recommends that you unzip the file contents to the `/tmp/MacInstaller` folder if you are running macOS 10.15.x and later. macOS prevents the create_package tool from running at locations like `Downloads`, `Documents`, and etc.
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_7.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 on user and edpa runs as root. Select **View All Processes** to view **edpa** if you are not logged on 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_7.pkg -target / -dumplog. Replace `/tmp/MacInstaller` with the path where you unzipped the agent installation package.
5	(Optional) Review information about the Mac agent installation.	What gets upgraded for DLP Agents on Mac endpoints

Upgrading DLP Agents on Mac endpoints silently

You can use a silent installation process by using systems management software (SMS) to upgrade DLP Agents to endpoints. You must always install the agent installation package from a local directory. If you do not install 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.

Generating agent installation packages

Packaging Mac agent upgrade files

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.

Related Links

What gets upgraded for DLP Agents on Mac endpoints on page 46

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 19: Mac agent components

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

Post-upgrade tasks

Learn about tasks you can perform after upgrading Symantec Data Loss Prevention.

Performing post-upgrade tasks

Verifying Symantec Data Loss Prevention operations

Migrating plug-ins

About securing communications between the Enforce Server and the database

About remote indexers

About updating the JRE to the latest version

Performing post-upgrade tasks

You must perform certain tasks after you finish upgrading.

Verifying Symantec Data Loss Prevention operations

Symantec Data Loss Prevention upgrade phases

Verifying Symantec Data Loss Prevention operations

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

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* at Related Documents for information about configuring incremental scans available.
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* available at Related Documents.

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/EnforceServer/15.7/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, custom plug-ins, custom scripts, previous version log files, or JAR files to the new version system location. You manually copy these files to the new location.

1. Locate the files you plan to move.

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

2. Copy the files to the following locations on the new version system:

   - Enforce Server: `/opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/plugins`
   - Detection server: `/opt/Symantec/DataLossPrevention/DetectionServer/15.7/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.

Table 20: Steps to secure communications between the Enforce Server and the database describes the process to secure communications between the Enforce Server and the database.

Table 20: Steps to secure communications between the Enforce Server and the database

Step	Action	More info
1	Generate the self-signed certificates using the orapki command-line utility that is provided with the Oracle database.	About orapki command line options Using orapki to generate the server certificate on the Oracle database
2	Configure the JDBC driver on the Enforce Server to use the TLS connection and port.	Configuring communication on the Enforce Server
3	Configure the server certificate on the Enforce Server.	Configuring the server certificate on the Enforce Server

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

Table 21: Orapki utility examples

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

Using orapki to generate the server certificate on the Oracle database

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

1. Stop the Oracle database.

   To stop the database, run the following command as a root user:

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

2. Log on as the Oracle User by running the following command:

   ```
   su - oracle
   ```

3. Go to the `oracle` directory by running the following command:

   ```
   cd /opt/oracle
   ```

4. Create the wallet directory by running the following command:

   ```
   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.

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.
8. 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.
9. 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)))
   ```

10. Navigate to the directory `$ORACLE_HOME/network/admin` and open the `tnsnames.ora` file.
11. 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))
    ```

12. Start all Oracle services.

    To view the services go to **Start > Control Panel > Administrative Tools > Computer Management**, and then expand **Services and Applications** and click **Services**.

13. Start the Oracle database by running the following command:

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

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

    ```
    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:

    ```
    su - oracle

    export ORACLE_SERVICE_NAME=protect

    sqlplus /nolog
    ```

SQL> conn sys/<password> as sysdba

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

```
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.

1. Locate the `jdbc.properties` file located at `/opt/Symantec/DataLossPrevention/EnforceServer/15.7/protect/config`.
2. Modify the following communication port and connection information:
   a) Update the **jdbc.dbalias.oracle-thin** line to use TCPS.
   b) Change the port number to 2484.

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

   ```
   jdbc.dbalias.oracle-thin=@(description=(address=(host=[oracle host name])
   (protocol=tcps)(port=2484))(connect_data=(SERVICE_NAME=protect))
   (SSL_SERVER_CERT_DN="CN=oracleserver"))
   ```

   NOTE

   If the server certificate on the Oracle database is signed by a public CA (instead of being self-signed), skip to step 5.
3. Add the certificate to the `cacerts` file that is located on the Enforce Server by completing the following steps:

a	Copy the `cert.txt` file to `/opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/lib/security`. Using orapki to generate the server certificate on the Oracle database
b	Change the directory by running the following command: `cd /opt/Symantec/DataLossPrevention/ServerJRE/1.8.0_202/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/ServerJRE/1.8.0_202/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

Related Links

About securing communications between the Enforce Server and the database on page 49

About remote indexers

The process of installing an EMDI, IDM, or EDM remote indexer is similar to installing a detection server, except that you use the `Indexers.zip`.

See the *Symantec Data Loss Prevention Administration Guide* at Related Documents for detailed information on installing and using a remote indexer.

About updating the JRE to the latest version

You use the JREMigrationUtility to update the JRE on each server, including the Enforce Server, detection server, indexers, the server that hosts a single-tier environment, and so on. If there is an off-cycle update to the OpenJRE, you can upgrade the JRE.

Steps to update the JRE

Prepare for updating the JRE by completing the following steps:

1. Download the latest version of the JREMigrationUtility. The utility is located in `Symantec_DLP_15.8.00000.19012_Platform_Lin-IN.zip for linux`, available from Product Downloads at the Broadcom Support Portal.
2. Install the OpenJRE.

   See Installing the OpenJRE for steps to install.

   NOTE

   The latest JRE improves LDAP security. However, the improved security may cause the SSL connection to Microsoft Active Directory to fail. If the SSL connection fails, add the following key to your SymantecDLPManager.conf file, then restart the Enforce Server:

   ```
   wrapper.java.additional.30 =-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
   ```

Installing the OpenJRE

These steps apply to Symantec Data Loss Prevention versions 15.1 and later.

1. Complete the following steps for Endpoint Servers where you plan to install OpenJRE.

   Applying this setting allows DLP Agents to connect to the Endpoint Server where the OpenJRE is installed.

   a) Go to **System > Servers and Detectors > Overview > Server/Detector Detail** screen, and click **Server Settings** for the Endpoint Server.

   b) Locate the **BoxMonitor.EndpointServerMemory** setting and enter the following string: `Djdk.security.allowNonCaAnchor=true`.

   c) Save your changes.

   d) Restart the Endpoint Server.

2. Obtain the latest supported version of OpenJRE from https://adoptopenjdk.net/.

   See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* available at the Tech Docs Portal.

3. Download the file (in tar.gz format) and move it to the Enforce Server and the detection servers.
4. Unzip the file to the JRE directory on the server.

   Symantec recommends that you use the following directory:

   `/opt/AdoptOpenJRE/jdk8u<version>-jre`

   The unzipping process completes the installation.

Updating the JRE to the latest version on Linux

During the update process, all Symantec Data Loss Prevention services are shut down and restarted automatically.

You can update the JRE on Linux using either of the following methods:

- Interactive mode
  Update the JRE using interactive mode
- Silent mode
  Update the JRE using silent mode

Update the JRE using interactive mode

During the migration process, all Symantec Data Loss Prevention services are shut down and restarted automatically.

1. Log on as a root user.
2. Create a directory called `/JREMigrationUtility`.
3. Move the `JREMigrationUtility.zip` file to `/JREMigrationUtility` directory.
4. Unzip `JREMigrationUtility.zip`.
5. Open a command prompt and navigate to the `/JREMigrationUtility/Migrator` directory.
6. Execute the following command:

   ```
   ./ServerJREMigrationUtility -jreDirectory=<JRE directory>
   ```

   Where <JRE directory> is the directory where the JRE is located (for example, `/opt/AdoptOpenJRE/jdk8u262-b10-jre`).
7. Choose the Symantec Data Loss Prevention version where you are upgrading the JRE. Enter the number corresponding with the version.
8. Press **Enter**.

   The migration process displays in the command line. You can find the migration log (`MigrationUtility.log`) in the `/JREMigrationUtility/Migrator` folder.

Update the JRE using silent mode

1. Log on as a root user.
2. Create directory called `/JREMigrationUtility`.
3. Move the `JREMigrationUtility.zip` file to `JREMigrationUtility` directory.
4. Unzip `JREMigrationUtility.zip`.
5. Open a command prompt and navigate to the `C:\JREMigrationUtility\Migrator` directory.
6. Execute the silent command.

   Silent mode parameters on Linux lists the parameters.

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

```
./ServerJREMigrationUtility -silent -sourceVersion=15.7 -jreDirectory=opt/AdoptOpenJRE/jdk8u262-b10-jre
```

Table 22: Silent mode parameters on Linux

Parameter	Description	Values
`-silent`	Enables silent mode.	N/A
`-sourceVersion`	Identifies the Symantec Data Loss Prevention version for which you want to upgrade the JRE version.	15.1, 15.5, or 15.7
`-jreDirectory`	Points to where the JRE installation is located. Use this parameter when you are migrating a JRE that is not provided by Symantec.	For example, `opt/AdoptOpenJRE`.

Reverting a JRE version to a previous release

You can revert the JRE to a previous version. The following steps use [previous_version] to refer to the previous JRE version.

NOTE

The process to revert the JRE temporarily shuts down then restarts services.

Reverting the JRE on Linux

1. Confirm that the Symantec Data Loss Prevention system is running.
2. Confirm that the JRE version you plan to revert to is installed on the Symantec Data Loss Prevention system.
3. Run the following command to point the ServerJREMigrationUtility to the previous JRE:

   ```
   ./ServerJREMigrationUtility -jreDirectory="<JRE directory>"
   ```

   Replace *`<JRE directory>`* with the directory where the previous JRE is located.

You can uninstall the unused JRE version, but you are not required to do so.

Starting and stopping services

About Symantec Data Loss Prevention services

About starting and stopping services on Linux

Starting an Enforce Server on Linux

Stopping an Enforce Server on Linux

Starting a detection server on Linux

Stopping a detection server on Linux

Starting services on single-tier Linux installations

Stopping services on single-tier Linux installations

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 23: Symantec Data Loss Prevention Enforce Server services

Service Name	Description
Symantec DLP Manager	Provides the centralized reporting and management services for Symantec Data Loss Prevention. See #unique_109/unique_109_Connect_42_task_1.
Symantec DLP Detection Server Controller	Controls the detection servers.
Symantec DLP Notifier	Manages communications between other DLP services and prevents transactional conflicts between the services and the database.
Symantec DLP Incident Persister	Writes the incidents to the database.

Increase the Max Memory

If you have more than 50 policies, 50 detection servers, or 50,000 agents, increase the `Max Memory` for this service from 2048 to 4096. You can adjust this setting in the `SymantecDLPManager.conf` file.

1. Open the `SymantecDLPManager.conf` file in a text editor.

   You can find this configuration file at `/opt/Symantec/DataLossPrevention/EnforceServer/Services`.

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

   ```
   wrapper.java.maxmemory = 4096
   ```

3. Save and close the file.

About starting and stopping services on Linux

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

- Starting an Enforce Server on Linux
- Stopping an Enforce Server on Linux
- Starting a detection server on Linux
- Stopping a detection server on Linux
- Starting services on single-tier Linux installations
- Stopping services on single-tier Linux installations

Starting an Enforce Server on Linux

Use the following procedure 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 SymantecDLPNotifierService start
```

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

```
service SymantecDLPManagerService start
service SymantecDLPIncidentPersisterService start
service SymantecDLPDetectionServerControllerService start
```

Related Links

Stopping an Enforce Server on Linux on page 58

Stopping an Enforce Server on Linux

Use the following procedure 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 commands:

```
service SymantecDLPDetectionServerControllerService stop
service SymantecDLPIncidentPersisterService stop
service SymantecDLPManagerService stop
service SymantecDLPNotifierService stop
```

Related Links

Starting an Enforce Server on Linux on page 58

Starting a detection server on Linux

Use the following procedure to start the Symantec Data Loss Prevention service 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 SymantecDLPDetectionServerService start
```

Related Links

Stopping a detection server on Linux on page 59

Stopping a detection server on Linux

Use the following procedure to stop the Symantec Data Loss Prevention service 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 SymantecDLPDetectionServerService stop
   ```

Related Links

Starting a detection server on Linux on page 58

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.

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 SymantecDLPNotifierService start
   ```

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

   ```
   service SymantecDLPManagerService start
   service SymantecDLPIncidentPersisterService start
   service SymantecDLPDetectionServerControllerService start
   service SymantecDLPDetectionServerService start
   ```

Related Links

Stopping services on single-tier Linux installations on page 59

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.

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 commands:

   ```
   service SymantecDLPDetectionServerService stop
   service SymantecDLPDetectionServerControllerService stop
   service SymantecDLPIncidentPersisterService stop
   service SymantecDLPManagerService stop
   service SymantecDLPNotifierService stop
   ```

Related Links

Starting services on single-tier Linux installations on page 59

Symantec Data Loss Prevention upgrade troubleshooting and recovery

Get information on troubleshooting issues and recovering data.

About troubleshooting Symantec Data Loss Prevention upgrade problems

Stop all Symantec Data Loss Prevention database sessions

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:

- Troubleshooting Enforce Server services
- Rolling back to the previous Symantec Data Loss Prevention release

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 `/var/log/Symantec/DataLossPrevention/EnforceServer/15.7/debug`.
- Symantec Data Loss Prevention operational logs are in `/var/log/Symantec/DataLossPrevention/<Enforce Server> or <Detection Server>/15.7/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.

Related Links

Reverting the Enforce Server to a previous release on page 61

Reverting a detection server to the previous release on page 62

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.

1. Stop all Symantec Data Loss Prevention services that are running on the version 15.7 Enforce Server.

   About Symantec Data Loss Prevention services

2. Disable all Symantec Data Loss Prevention services that are running on the version 15.7 Enforce Server.

3. Stop all the Oracle services.

4. Restore Symantec Data Loss Prevention services if you are reverting to version 15.5 or later. For version 15.1 and earlier, see step 5.

   Symantec Data Loss Prevention version 15.5 and later services are backed up during the migration process. You must move the service files to the previous release `Services` folder.

   - Locate the backed up services at the following location:
     `/opt/Symantec/DataLossPrevention/EnforceServer/vv.u/Protect/backup/service-<date>-<time>`
     Replace vv.u with the previous version and <date>-<time> with the date and time the migration process completed.
   - Copy the following services:
     - `SymantecDLPNotifier.conf`
     - `SymantecDLPManager.conf`
     - `SymantecDLPIncidentPersister.conf`
     - `SymantecDLPDetectionServerController.conf`
   - Paste the services to the following location:
     `/opt/Symantec/DataLossPrevention/EnforceServer/Services`

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

   Consult the 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:

```
chown -R oracle:oinstall protect
```

6. Restart all the Oracle services.

   Consult the Oracle documentation for more information.
7. Enable the services on the previous Symantec Data Loss Prevention version.
8. 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.

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

   Symantec Data Loss Prevention services are backed up during the migration process. You must move the service files to the previous release `Services` folder.

   - Locate the backed up services at the following location:
     `/opt/Symantec/DataLossPrevention/DetectionServer/vv.u/Protect/backup/service-<date>-<time>`
     Replace vv.u with the previous version and <date>-<time> with the date and time the migration process completed.
   - Copy the `SymantecDLPDetectionServer.conf` services.
   - Paste the service to the following location:
     `/opt/Symantec/DataLossPrevention/DetectionServer/Services`
3. Enable the services on the previous Symantec Data Loss Prevention version.
4. Start services on the previous Symantec Data Loss Prevention version.

Related Links

Rolling back to the previous Symantec Data Loss Prevention release on page 60
Reverting the Enforce Server to a previous release on page 61

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 files such as the `CryptoMasterKey.properties` file and keystore files, which are required to connect Symantec Data Loss Prevention to an existing DLP database.

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 15.7 installer.

Creating the Enforce Reinstallation Resources file on Linux

1. Locate the ReinstallationResourcesUtility at `/opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/bin`.
2. Generate an Enforce Reinstallation Resources file by running the following command:

   ```
   ./ReinstallationResourcesUtility export /opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect /opt/EnforceReinstallationResources.zip
   ```

3. Identify this new `EnforceReinstallationResources.zip` when reinstalling Symantec Data Loss Prevention from your backup version.

   Include the following parameters (in addition to other required parameters):

   ```
   reinstallationResourceFile="/opt/EnforceReinstallationResources.zip"
   ```

   Creating the Enforce Reinstallation Resources file

Uninstalling a server from a Linux system

The uninstallation process deletes all files and directories created by the installer. Complete the following backup tasks before uninstalling a server:

- Ensure that you have backed up all keystore files.
  See Backing up keystore files on Linux.
- Run the Reinstallation Resources Utility to create a backup of the `CryptoMasterKey.properties` file and Enforce Server keystore files.
  Creating the Enforce Reinstallation Resources file

Run the following uninstallation command to remove all servers and components for version 15.7:

```
rpm -e $(rpm -qa "symantec-dlp-15-7*")
```

Applying a Maintenance Pack

Maintenance Packs can only be applied to an already installed version of Symantec Data Loss Prevention. For example, a maintenance pack for 15.7 can only be applied to Symantec Data Loss Prevention 15.7 (new or upgraded installation).

Before applying a maintenance pack or installing Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about system requirements available at: Related Documents.

Steps to apply a maintenance pack on Linux servers

The following table describes the high-level steps that are involved in applying a Symantec Data Loss Prevention maintenance pack to a Linux server. Each step is described in more detail elsewhere in this chapter, as indicated.

Before you apply a maintenance pack, 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. You can use the file to rollback to a previous version.

See the *Symantec Data Loss Prevention Upgrade Guide for Linux* at Related Documents.

Table 24: Steps to apply the maintenance pack on Linux

Step	Action	Description
1	Download and extract the upgrade software.	Downloading and extracting the maintenance pack software for Linux servers
2	Confirm that all users are logged out of the Enforce Server administration console.	If users are logged in during the maintenance pack application process, subsequent logins fail during the End User Licensing Agreement confirmation.
3	Apply the maintenance pack to the Enforce Server.	Updating the Enforce Server on Linux The process to apply the maintenance pack to a single-tier installation omits the detection server update step. Updating a single-tier system on Linux
4	Apply the maintenance pack to the detection server.	Updating the detection server on Linux

Downloading and extracting the maintenance pack software for Linux servers

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.

Copy the ZIP files into a directory on a system that is accessible to you. The root directory where you move the files is referred to as the `DLPDownloadHome` directory.

Choose from the following files based on your current installation:

- Apply the maintenance pack to the Enforce Server: `EnforceServer.zip`
- Apply the maintenance pack to the detection server: `DetectionServer.zip`
- Update a single-tier installation: `SingleTierServer.zip`

Updating the Enforce Server on Linux

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

These instructions assume that Symantec Data Loss Prevention 15.7 is installed and that the `EnforceServer.zip` file has been copied into the `/opt/temp` directory on the Enforce Server computer.

1. Log on as root to the Enforce Server system.
2. Navigate to the directory where you copied the `EnforceServer.zip` file. (`/opt/temp`)
3. Unzip the file to the same directory.
4. Install the maintenance pack by running the following command:

   ```
   ./install.sh -t enforce
   ```

   Parameters for install.sh

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

5. Run the Update Configuration utility by running the following command:

   ```
   cd "/opt/Symantec/DataLossPrevention/EnforceServer/15.7/Protect/install"
   ```

   ```
   ./EnforceServerUpdateConfigurationUtility
   ```

   NOTE

   You can install the maintenance pack silently by running the following command:

   ```
   ./EnforceServerUpdateConfigurationUtility -silent -ORACLE_HOME=/opt/oracle/
   product/12.2.0.1/db_1 -oraclePassword=<ORACLE PASSWORD>
   ```

   where <ORACLE PASSWORD> is the database password used for Symantec Data Loss Prevention.

   During the update process, services shut down, then restart automatically. You can review the update log file `EnforceServerUpdateConfigurationUtility.log` located at `/var/log/Symantec/DataLossPrevention/EnforceServer/15.7/debug`.

Updating the detection server on Linux

The instructions that follow describe how to apply the maintenance pack to a detection server on a Linux computer.

These instructions assume that Symantec Data Loss Prevention 15.7 is installed and that the `DetectionServer.zip` file has been copied into the `/opt/temp/` directory on the server computer.

1. Log on as root to the system where the detection server is installed.
2. Navigate to the directory where you copied the `DetectionServer.zip` file. (`/opt/temp`)
3. Unzip the file to the same directory.
4. Apply the maintenance pack to the detection server by running the following command:

   ```
   ./install.sh -t detection
   ```

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

   Parameters for install.sh

Updating a single-tier system on Linux

The instructions that follow describe how to apply a the maintenance pack to a single-tier installation on a Linux computer.

These instructions assume that Symantec Data Loss Prevention 15.7 is installed and that the `SingleTierServer.zip` file has been copied into the `/opt/temp` directory on the computer.

1. Log on as root to the Enforce Server system.
2. Navigate to the directory where you copied the `SingleTierServer.zip` file. (`/opt/temp`)
3. Unzip the file to the same directory.
4. Apply the maintenance pack to the single-tier installation by running the following command:

   ```
   ./install.sh -t singletier
   ```

   NOTE

   If you use YUM to install, you cannot override the default relocatable roots where Symantec Data Loss Prevention is installed.

   Parameters for install.sh

5. Run the Update Configuration utility by running the following command:

   ```
   cd "/opt/Symantec/DataLossPrevention/SingleTierServer/15.7/Protect/install"
   ```

   ```
   ./SingleTierServerUpdateConfigurationUtility
   ```

   NOTE

   You can install the maintenance pack silently by running the following command:

   ```
   ./SingleTierServerUpdateConfigurationUtility -silent -ORACLE_HOME=/opt/oracle/
   product/12.2.0.1/db_1 -oraclePassword=<ORACLE PASSWORD>
   ```

   where <ORACLE PASSWORD> is the database password used for Symantec Data Loss Prevention 15.7.

   During the update process, services shut down, then restart automatically. You can review the update log file `SingleTierServerUpdateConfigurationUtility.log` located at /var/log/Symantec/DataLossPrevention/SingleTierServer/15.7/debug/.

Copyright statement

Copyright statement

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

Symantec™

A Division of Broadcom