Symantec™ Data Loss Prevention Upgrade Guide for Windows

Version 15.5

Last updated: 16 September 2019

Symantec

Symantec Data Loss Prevention Upgrade Guide for Windows

Documentation version: 15.5f

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Preparing to upgrade Symantec Data Loss Prevention

This chapter includes the following topics:

About updates to the *Symantec Data Loss Prevention Upgrade Guide*

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

Subscribe to the article at the Support Center to be notified when there are updates.

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

Table 1-1 Change history for the *Symantec Data Loss Prevention Upgrade Guide for Windows*

Date	Change description
16 September 2019	Minor stylistic change to Update Readiness tool topic. Clarified command for running the migration utility on Windows.
22 April 2019	Corrected step for setting server bindings when upgrading detection servers. Removed reference to `basepatch.msp` from procedures about applying a maintenance pack.
6 March 2019	Reinstated cross-reference link to "Starting an Enforce Server on Windows" topic (inadvertently dropped in previous release), minor stylistic changes.
5 February 2019	Clarified Upgrade Readiness tool preparation and usage. Other minor stylistic changes.
11 January 2019	Corrected path to the Single-Tier Server migration utility.

About preparing to upgrade Symantec Data Loss Prevention

To review the new features for Symantec Data Loss Prevention 15.5, see the *What's New and What's Changed in Symantec Data Loss Prevention 15.5*: http://www.symantec.com/docs/DOC10601

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

Symantec Data Loss Prevention 15.5 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 15.5, 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 15.5 detection servers.

See "Supported upgrade backward compatibility for agents and servers" on page 22.

See "Upgrade requirements and restrictions" on page 24.

Back up your database before any upgrade. See the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide* for more information.

Symantec Data Loss Prevention upgrade phases

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

Table 1-2 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 15.5 Release Notes* at http://www.symantec.com/docs/DOC10600 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 http://www.symantec.com/docs/DOC10601 for information about new and changed features in Symantec Data Loss Prevention 15.5. See "About the minimum system requirements for upgrading to the current release" on page 21. See "About the requirement for language pack upgrades" on page 24.

Table 1-2 Symantec Data Loss Prevention upgrade phases *(continued)*

Phase	Action	Description
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.	See "Preparing your system for the upgrade" on page 25.
3	Download and extract the version 15.5 software.	See "Downloading and extracting the upgrade software" on page 30.
4	Upgrade the Enforce Server, which includes the following steps: ■ Install the Java Runtime Environment. ■ Install the version 15.5 Enforce Server. ■ Run the Update Readiness tool. If you find issues, fix them before you migrate your data to version 15.5. ■ Migrate the previous version to the version 15.5 Enforce Server.	See "Migrating previous version data to a new Enforce Server installation" on page 31. See "Migrating previous version data to a new single-tier installation" on page 44.
5	Upgrade detection servers, which includes the following steps: ■ Install the Java Runtime Environment. ■ Install the version 15.5 detection server. ■ Migrate the previous version to the version 15.5 detection server.	See "Migrating a previous version detection server to the latest version" on page 38.
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 15.5 detection servers. See "Supported upgrade backward compatibility for agents and servers" on page 22.	See "About Symantec Data Loss Prevention Agent upgrades" on page 54.
7	Upgrade any scanners.	See "Upgrading your scanners" on page 52.

Table 1-2 Symantec Data Loss Prevention upgrade phases *(continued)*

Phase	Action	Description
8	Complete the required and optional post-upgrade tasks.	See "Performing post-upgrade tasks" on page 73.

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 15.5:

Table 1-3 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*: http://www.symantec.com/docs/DOC10713
2	Run the Update Readiness tool to confirm that the Oracle database is ready to upgrade to Symantec Data Loss Prevention version 15.5.	See "Checking the database update readiness" on page 13.
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.	See "Switching from `SID` to `SERVICE_NAME`" on page 19.
4	Set ORACLE_HOME and PATH variables.	See "Setting ORACLE_HOME and PATH variables" on page 20.
5	Confirm the database user has permissions to connect to the Enforce Server.	See "Confirming the Oracle database user permissions" on page 21.

See "Preparing your system for the upgrade" on page 25.

Checking the database update readiness

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

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

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

Table 1-4 lists tasks you complete to run the tool.

Table 1-4 Using the Update Readiness tool

Step	Task	Details
1	Prepare to run the Update Readiness tool.	See "Preparing to run the Update Readiness tool" on page 13.
2	Create the Update Readiness tool database account.	See "Creating the Update Readiness tool database account" on page 15.
3	Run the tool.	See "Running the Update Readiness tool at the command line" on page 16.
4	Review the update readiness results.	See "Reviewing update readiness results" on page 18.

Preparing to run the Update Readiness tool

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

To prepare the Update Readiness tool

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

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

Symantec recommends that you download the tool to the *DLPDownloadHome*\DLP\15.5\ directory.

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

---

2 Log on as Administrator to the database server system.

3 Confirm the following if you are running a three-tier deployment:

- That 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.
- That 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`.

4 Stop Oracle database jobs if your database has scheduled jobs.

See "Stopping Oracle database jobs" on page 15.

5 Unzip the tool, then copy the contents of the unzipped folder to the following location. Do not unzip the tool as a folder to this location: The contents of the tool folder must reside directly in the `URT` folder as specified:

```
c:\Program
Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\Migrator\URT\
```

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

See "Checking the database update readiness" on page 13.

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.

To unschedule jobs

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.

To create the new Update Readiness tool database account

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

```
sqlplus /nolog
```

3. Run the `oracle_create_user.sql` script:

```
SQL> @oracle_create_user.sql
```

4. At the **Please enter the password for sys user** prompt, enter the password for the SYS user.
5. At the **Please enter Service Name** prompt, enter a user name.
6. At the **Please enter required username to be created** prompt, enter a name for the new upgrade readiness database account.
7. At the **Please enter a password for the new username** prompt, enter a password for the new upgrade readiness database account.

   Use the following guidelines to create an acceptable password:

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

   Store the user name and password in a secure location for future use. You use this user name and password to run the Update Readiness tool.
8. As the database sysdba user, grant permission to the Symantec Data Loss Prevention *schema user name* for the following database objects:

```
sqlplus sys/[sysdba 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];
```

See "Preparing to run the Update Readiness tool" on page 13.

See "Checking the database update readiness" on page 13.

Running the Update Readiness tool at the command line

You can run the Update Readiness tool from the command prompt on the Enforce Server host computer.

Note: The steps assume that you have logged on as the administrator user to the computer on which you intend to run the Update Readiness tool.

To run the Update Readiness tool

1. Open a command prompt window.
2. Go to the `URT` directory:

   ```
   c:\Program
   Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\Migrator\URT
   ```

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

```
"C:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181\bin\java" UpdateReadinessTool
--username <schema user name>
--password <password>
--readiness_username <readiness_username>
--readiness_password <readiness_password>
--sid <database_system_id>
[--quick]
```

The following table identifies the commands:

<schema user name>	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 you created. See "Creating the Update Readiness tool database account" on page 15.
<readiness_password>	The password for the Update Readiness tool database account user.
<database_system_id>	The database system ID (SERVICE_NAME), typically "protect."
`[--quick]`	The optional command 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.

See "Preparing to run the Update Readiness tool" on page 13.

See "Reviewing update readiness results" on page 18.

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.

To run the Update Readiness tool

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.

   See "Preparing to run the Update Readiness tool" on page 13.
3. Enter the Update Readiness tool database account user credentials.

   Warning: Do not enter the protect user database credentials. Entering credentials other than the Update Readiness tool database account overwrites the Symantec Data Loss Prevention database.

   See "Creating the Update Readiness tool database account" on page 15.
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.

See "Reviewing update readiness results" on page 18.

See "Checking the database update readiness" on page 13.

Reviewing update readiness results

After you run the Update Readiness tool, the tool returns test results in a log file. Table 1-5 lists the results summarized in the log file.

Table 1-5 Update Readiness results

Status	Description
Pass	Items that display under this section are confirmed and ready for update.

Table 1-5 Update Readiness results *(continued)*

Status	Description
Warning	If not fixed, items that display under this section may prevent the database from upgrading properly.
Error	These items prevent the upgrade from completing and must be fixed.

See "Checking the database update readiness" on page 13.

Switching from SID to SERVICE_NAME

Before you upgrade to Symantec Data Loss Prevention 15.1 you switch the Oracle SID to SERVICE_NAME. 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*. This guide is available online at the Symantec Support Center at:

http://www.symantec.com/docs/DOC9258

Switch from SID to SERVICE_NAME

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

Switching from SID to SERVICE_NAME

1. Locate the tnsnames.ora file.

   The file is located at %ORACLE_HOME%\network\admin on Windows.

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 = 127.0.0.1)(PORT = 1521)))
        (CONNECT_DATA =
        (SERVICE_NAME = protect)
        )
    )
```

Register the service name

Registering 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 protect users 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 process.

To set the ORACLE_HOME and PATH variable on Windows

1. Log on as a domain user.
2. In the command prompt, run the following command to set the ORACLE_HOME variable. Confirm your Oracle version and installation path before setting this variable. For example:

```
set ORACLE_HOME=c:\oracle\product\12.2.0.1\db_1
```

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

```
set 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.

To confirm the Oracle database user permissions

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. Exit SQL*Plus:

```
SQL> exit
```

About the minimum system requirements for upgrading to the current release

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

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

Note: These numbers refer to the free disk space that is needed for the upgrade process, not the disk space that is required for server operation. For server disk space, operating system, and other requirements, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*: http://www.symantec.com/docs/DOC10602

See "About preparing to upgrade Symantec Data Loss Prevention" on page 9.

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 15.5, 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 15.5. 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 15.5. Ideally, you will only be on one of the following backward-compatible scenarios for a limited time as you upgrade all servers and agents to version 15.5.

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 15.5 detection servers.

Table 1-6 Supported backward compatibility for agent upgrades

Enforce Server version	Endpoint Server version	Symantec DLP Agent version	Results
15.5	15.5	15.5	All incidents are sent to the Enforce Server. Policy and configuration updates can be sent to the Endpoint Servers and agents.
15.5	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.
15.5	15.5	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 15.5.
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.

Table 1-6 Supported backward compatibility for agent upgrades *(continued)*

Enforce Server version	Endpoint Server version	Symantec DLP Agent version	Results
15.5	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* for information about acquiring and adding updated language packs.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 9.

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 15.5. You cannot restart Network Discover scans until at least one Network Discover detection server has been upgraded to version 15.5.
- If a version 14.x or 15.0 detection server stops (shuts down) after you have upgraded the Enforce Server to version 15.5, you must upgrade that detection server to version 15.5 before it can restart.
- After you upgrade the Enforce Server to version 15.5, any configuration changes that you make have no effect on version 12.x detection servers.
- After you complete the upgrade, do not modify the host name or IP address of a detection server to point to a different detection server. Detection servers use the original configured IP address or host name to maintain and report server-level statistics.
- Restart the `SymantecDLPDetectionServerControllerService` service to verify the upgraded detection server versions in the Enforce Server administration console.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 9.

Preparing your system for the upgrade

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

See "Upgrade requirements and restrictions" on page 24.

See "About external storage for incident attachments" on page 25.

See "Preparing the Oracle database for a Symantec Data Loss Prevention upgrade" on page 12.

See "Creating the Update Readiness tool database account" on page 15.

See "Creating the Enforce Reinstallation Resources file" on page 92.

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

See "About the minimum system requirements for upgrading to the current release" on page 21.

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 recommend these best practices:

- If you choose to store your incident attachments on the Enforce Server host computer, do not place your storage directory under the `\Data Loss Prevention\` 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 15.5, 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.

Preparing your environment for Microsoft Rights Management file monitoring

You must complete prerequisites before enabling Microsoft Rights Management (RMS) file monitoring. The following prerequisites apply to Azure RMS or Active Directory (AD) RMS.

Prepare the AD RMS environment for RMS monitoring

Complete the following steps to prepare your AD RMS environment for monitoring:

1. Confirm that the latest AD RMS client is installed.
2. Confirm that the AD RMS account has Read and Execute permissions to access `ServerCertification.asmx`. For additional details, refer to the Microsoft Developer Network article: https://msdn.microsoft.com/en-us/library/mt433203.aspx.
3. Confirm that the AD RMS superuser group and Service Group both have Read and Execute permissions.
4. Add each detection server to the AD RMS domain.
5. Complete the following to change the previous Symantec Data Loss Prevention version service user to a domain user that has access to the AD RMS superuser group.
   - Shut down all services on the detection server before updating the service user.
   - Run the `ChangeServiceUser.exe` utility to change the service user:

```
C:\Program Files\Symantec\DataLossPrevention\Protect\bin>ChangeServiceUser.exe
USAGE: ChangeServiceUser.exe [installation directory]
[new service user username] [new service user password]
```

```
Parameters:
    [new service user password] is optional.

C:\Program Files\Symantec\DataLossPrevention\Protect\bin>ChangeServiceUser.exe
C:\Program Files\Symantec\DataLossPrevention\ [AD RMS domain name]\[super user username]
[super user password]
```

After running the script, the command prompt displays the change status, including the service user change status.

6 Start all services after updating the service user.

Prepare the Azure RMS environment for RMS monitoring

Complete the following steps to prepare your Azure RMS environment for RMS monitoring:

1 Confirm that the latest Azure RMS client is installed.

2 Create a local or domain user on each detection server that can access the Azure RMS.

After you upgrade the detection server, you enable the Microsoft Rights Management plug-in to complete the process to monitor Microsoft Rights Management files. See "Enabling Microsoft Rights Management file monitoring" on page 74.

Chapter 2

Upgrading Symantec Data Loss Prevention to a new release

This chapter includes the following topics:

Upgrading Symantec Data Loss Prevention

After preparing your system for the upgrade, you are ready to perform the upgrade itself. The following table describes the high-level steps that are involved in upgrading Symantec Data Loss Prevention. Each step is described in more detail elsewhere in this chapter, as indicated.

Note: If you are upgrading your system and you have deployed Exact Data Matching (EDM) profiles and policies, there is a specific upgrade path you need to perform so that your profiles and policies update properly. See "Updating EDM indexes to the latest version" in the *Symantec Data Loss Prevention Administration Guide* or Updating EDM indexes to the latest version in the Help.

Table 2-1 Upgrading Symantec Data Loss Prevention

Step	Action	Description
1	Download and extract the upgrade software.	See "Downloading and extracting the upgrade software" on page 30.
2	Confirm that your existing Enforce Server and detection servers are running.	See "Verifying that the Enforce Server and the detection servers are running" on page 52.
3	Close all files and folders in your `\Program Files\Symantec\Data Loss Prevention\` directory.	Ensure that all folders and files in your *Data Loss Prevention* directory are closed and unlocked. The upgrader requires access to all *Data Loss Prevention* folders and files during the upgrade process.
4	Install the Java Runtime Environment on the Enforce Server.	See "Installing the Java Runtime Environment on the Enforce Server" on page 31.
5	Prepare the Update Readiness tool.	See "Preparing to run the Update Readiness tool" on page 13. See "Creating the Update Readiness tool database account" on page 15.
6	Install the version 15.5 Enforce Server.	See "Installing an Enforce Server" on page 32.
7	Run the Update Readiness tool on the version 15.5 Enforce Server.	See "Running the Update Readiness tool from the Enforce Server administration console" on page 18. See "Running the Update Readiness tool at the command line" on page 16.
8	Migrate the previous version to the version 15.5 Enforce Server.	See "Running the Migration Utility on the Enforce Server" on page 37.
9	Install the Java Runtime Environment on the detection server.	See "Installing a detection server" on page 39.

Table 2-1 Upgrading Symantec Data Loss Prevention *(continued)*

Step	Action	Description
10	Install the version 15.5 detection servers.	See "Installing a detection server" on page 39.
11	Migrate the previous version to the version 15.5 detection servers.	See "Running the Migration Utility on a detection server" on page 43.
12	(Optional) Apply the updated agent configuration to Endpoint Prevent detection servers.	See "Applying the updated configuration to Endpoint Prevent servers" on page 52.
13	(Optional) Update Symantec DLP Agents.	See "About Symantec Data Loss Prevention Agent upgrades" on page 54.
14	(Optional) Update any scanners.	See "Upgrading your scanners" on page 52.
15	Upgrade WinPcap (Network Monitor deployments only).	
16	Reindex IDM and EDM profiles.	

Downloading and extracting the upgrade software

To download the upgrade software

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

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

To extract the ZIP files

1. Extract the contents of the `Symantec_DLP_15.5_Platform_Win-IN.zip` file.
2. Extract the contents of the `Symantec_DLP_15.5_Agent_Win-IN.zip` file.
3. Extract the contents of the `Symantec_DLP_15.5_Agent_Mac-IN.zip` file.
4. Note where you saved the MSI and PKG files so you can quickly find them later.

See "Symantec Data Loss Prevention upgrade phases" on page 10.

Migrating previous version data to a new Enforce Server installation

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

To upgrade the Enforce Server to the latest version

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

   See "Installing the Java Runtime Environment on the Enforce Server" on page 31.

2. Run the Update Readiness tool.

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

   See "Checking the database update readiness" on page 13.

3. Install the version 15.5 Enforce Server.

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

   See "Installing an Enforce Server" on page 32.

4. Migrate the previous version to the version 15.5 Enforce Server.

   Migrating data—in addition to moving data to the new system—moves data, configurations, and custom files (which includes data profiles, plug-ins, and incidents) to the 15.5 instance. The migration utility also stops previous version services and starts new version services.

The process to migrate data does not move all plug-ins.See "Migrating plug-ins" on page 75.

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.

To install the JRE

1. Copy `ServerJRE.msi` from your *`DLPDownloadHome`*`\DLP\New_Installs\Release` directory to the computer where you plan to install the Enforce Server (for example, move the file to `c:\temp`).
2. Log on (or remote logon) as Administrator to the Enforce Server system on which you intend to install Enforce.
3. Run the `ServerJRE.msi` file to display the **Symantec Data Loss Prevention Server JRE Setup** dialog.
4. Click **Next**.

5 After you review the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.

6 In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**.

Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.

7 Click **Install** to begin the installation process.

8 Click **Finish** to complete the process.

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server on a Windows computer in a two- or three-tier environment. The steps to install the Enforce Server in a single-tier environment are different. See "Installing a single-tier server" on page 45.

These instructions assume that the `EnforceServer.msi` file and license file have been copied into the `c:\temp` directory on the Enforce Server computer.

Note: Enter directory names, account names, passwords, IP addresses, and port numbers that you create or specify during the installation process using standard 7-bit ASCII characters only. Extended (hi-ASCII) and double-byte characters are not supported.

Using the graphical user interface method to install does not generate log information. To generate log information, run the installation using the following command:

```
msiexec /i EnforceServer.msi /L*v c:\enf_data\enforce_install.log
```

You can complete the installation using Silent Mode. Enter values with information specific to your installation for the following:

Table 2-2 Enforce Server Silent Mode installation parameters

Command	Description
`INSTALLATION_DIRECTORY`	Specifies where the Enforce Server is installed. The default location is `C:\Program Files\Symantec\DataLossPrevention`.

Table 2-2 Enforce Server Silent Mode installation parameters *(continued)*

Command	Description
DATA_DIRECTORY	Defines where Symantec Data Loss Prevention stores files that are updated while the Enforce Server is running (for example, logs and licenses). The default location is `\ProgramData\Symantec\DataLossPrevention\EnforceServer\`. **Note:** If you do not use the default location, you must indicate a folder name for the data directory. If you set the data directory to the drive root (for example `c:\` or `e:\`) you cannot successfully uninstall the program.
JRE_DIRECTORY	Specifies where the JRE resides.
FIPS_OPTION	Defines whether to disable (**Disabled**) or enable (**Enabled**) FIPS encryption.
SERVICE_USER_OPTION	Defines whether to create a new service user by entering **NewUser** or using an existing one by entering **ExistingUser**.
SERVICE_USER_USERNAME	Defines a name for the account that is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.”
SERVICE_USER_PASSWORD	Defines the password for the account that is used to manage Symantec Data Loss Prevention services.
ORACLE_HOME	Defines the Oracle Home Directory. For example, use `c:\oracle\product\12.2.0.1\db_1` to define the home directory if you use the Oracle 12.2.0.1 database.
ORACLE_HOST	Defines the IP address of the Oracle server computer.
ORACLE_PORT	Defines the Oracle listener port (typically 1521).
ORACLE_USERNAME	Defines the Symantec Data Loss Prevention database user name.
ORACLE_PASSWORD	Defines the Symantec Data Loss Prevention database password.
ORACLE_SERVICE_NAME	Defines the database SERVICE_NAME (typically “protect”).
EXTERNAL_STORAGE_OPTION	Defines whether incident attachments are stored in the database (**Database**) or in external storage (**ExternalStorage**).
EXTERNAL_STORAGE_DIRECTORY	Defines the path where you plan to store incident attachments.
ADDITIONAL_LOCALE	Defines an additional locale for use by individual users.
ENFORCE_ADMINISTRATOR_PASSWORD	Defines the Enforce Server administration console password. The Enforce Server administration console passport must be at least eight characters long. This parameter is required during the migration.

The following is an example of what the completed command might look like. The command you use differs based on your implementation requirements. Using the following command as-is may cause the installation to fail.

```
msiexec /i EnforceServer.msi /qn /norestart /lv d:\EnforceServer.log
INSTALLATION_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention"
DATA_DIRECTORY="C:\ProgramData\Symantec\DataLossPrevention\EnforceServer"
JRE_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181"
FIPS_OPTION=Disabled
SERVICE_USER_OPTION=ExistingUser
SERVICE_USER_USERNAME=protect
SERVICE_USER_PASSWORD=Password
ORACLE_HOST=xxx.xxx.xxx.xxx
ORACLE_PORT=1521
ORACLE_USERNAME=protect
ORACLE_PASSWORD=Password
ORACLE_SID=protect
EXTERNAL_STORAGE_OPTION=Database
ENFORCE_ADMINISTRATOR_PASSWORD=Password
```

To install an Enforce Server

1. Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.
2. (Optional) Change the location where Symantec Data Loss Prevention stores files.
3. Log on (or remote logon) as Administrator to the Enforce Server system where you intend to run the Migration Utility.
4. Go to the folder where you copied the `EnforceServer.msi` file (`c:\temp`).

   Note: Using the graphical user interface method to install does not generate log information. To generate log information, run the installation using the following command:

   ```
   msiexec /i EnforceServer.msi /L*v c:\enf_data\enforce_install.log
   ```

   After you complete the Enforce Server installation, you can find the log file at `c:\enf_data`.

   ---

5. Double-click `EnforceServer.msi` to execute the file, and click **OK**.
6. In the **Welcome** panel, click **Next**.
7. After you review the license agreement, select **I accept the agreement**, and click **Next**.

8 In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**. The default installation directory is:

```
c:\Program Files\Symantec\DataLossPrevention\
```

Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.

9 In the **JRE Directory** panel, accept the default JRE location (or click **Browse** to locate it), and click **Next**.

10 In the **FIPS Cryptography Mode** panel, select whether to disable or enable FIPS encryption.

11 In the **Service User** panel, select one of the following options.

- **New Users**: Select this option to create the Symantec Data Loss Prevention system account user name and password and confirm the password. This account is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.” New service user accounts must be admin local accounts.

  Note: The password you enter for the System Account must conform to the password policy of the server. For example, the server may require all passwords to include special characters.

- **Existing Users**: Select this option to use an existing local or domain user account.

Click **Next**.

12 (Optional) If you opted to create a new service user, enter the new account name and password. Confirm the password, then click **Next**.

13 (Optional) If you opted to use an existing domain user account, enter the account name and password. The user name must be in ***DOMAIN**username*** format.

14 In the **Oracle Database** panel, enter details about the Oracle database server. Specify one of the following options in the **Oracle Database Server** field:

Host Enter host information based on your Symantec Data Loss Prevention installation:

- Single- and two-tier installation (Enforce and Oracle servers on the same system): The Oracle Server location is **127.0.0.1**.
- Three-tier installation (Enforce Server and Oracle server on different systems): Specify the Oracle server host name or IP address. To install into a test environment that has no DNS available, use the IP address of the Oracle database server.

Port	Enter the **Oracle Listener Port**, or accept the default.
Service Name	Enter the database SERVICE_NAME (typically “protect”).
Username	Enter the Symantec Data Loss Prevention database user name.
Password	Enter the Symantec Data Loss Prevention database password.

If your Oracle database is not the correct version, you are warned and offered the choice of continuing or canceling the installation. You can continue and upgrade the Oracle database later.

Note: Symantec Data Loss Prevention requires the Oracle database to use the AL32UTF8 character set. If your database is configured for a different character set, you are notified and the installation is canceled. Correct the problem and re-run the installer.

---

15 Click **Next** to display the **Enable external storage for incident attachments** panel.

16 If you choose to store your incident attachments externally, select the **Enable external storage for incident attachments** box and enter the path or browse to your external storage directory.

17 In the **Additional Locale** panel, select an alternate locale, or accept the default of None, and click **Next**.

Locale controls the format of numbers and dates, and how lists and reports are alphabetically sorted. If you accept the default choice of None, English is the locale for this Symantec Data Loss Prevention installation. If you choose an alternate locale, that locale becomes the default for this installation, but individual users can select English as a locale for their use.

See the *Symantec Data Loss Prevention Administration Guide* for more information on locales.

18 Click **Install**.

The installation process can take a few minutes. The installation program window may persist for a while during the startup of the services. After a successful installation, a completion notice displays.

Note: Symantec Data Loss Prevention services are created but remain in a disabled state until you run the Enforce Server Migration Utility.

See “Running the Migration Utility on the Enforce Server” on page 37.

---

19 Restart any antivirus, pop-up blocker, or other protection software that you disabled before starting the Symantec Data Loss Prevention installation process.

20 Run the Upgrade Readiness tool to confirm that the Oracle database is ready to be migrated to the new instance.

See "Checking the database update readiness" on page 13.

21 Verify that the Enforce Server is properly installed.

Running the Migration Utility on the Enforce Server

Before you run the Migration Utility, run the Update Readiness tool to confirm that the database is ready for migration.

See "Checking the database update readiness" on page 13.

There are two ways to complete the migration: you can use silent mode or interactive mode. See "To migrate data from a previous Enforce Server version to version 15.5 using interactive mode" on page 37.

To migrate data from a previous Enforce Server version to version 15.5 using silent mode

- You can complete the migration using Silent Mode. Run the following command in an elevated command prompt:

```
EnforceServerMigrationUtility
-silent
-sourceInstallation="previous version path"
```

Where *previous version path* represents where the previous, active version is installed (for example, `C:\SymantecDLP)`.

To migrate data from a previous Enforce Server version to version 15.5 using interactive mode

1 Log on (or remote logon) as Administrator to the Enforce Server system where you intend to run the Migration Utility.

2 Use the command prompt to navigate to the following directory:

```
C:\Program
Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\Migrator
```

3 Run the Migration Utility: `EnforceServerMigrationUtility`.

4 Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.

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.

Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.5 installation. If you uninstall the previous version, the service_user is removed.

---

5 If migration fails, review the Enforce Server `MigrationUtility.log` located at `C:\ProgramData\Symantec\DataLossPrevention\EnforceServer\15.5\logs\debug\` for more details.

Migrating a previous version detection server to the latest version

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

To upgrade a detection server to the latest version

1 Install the Java Runtime Environment on the detection server.

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

See "Installing the Java Runtime Environment on a detection server" on page 38.

2 Install the version 15.5 detection servers.

See "Installing a detection server" on page 39.

3 Migrate the previous version to the version 15.5 detection servers.

See "Running the Migration Utility on a detection server" on page 43.

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.

To install the JRE

1 Log on as Administrator to the computer on which you plan to install the detection server.

2 Copy `ServerJRE.msi` from your *`DLPDownloadHome`*`\DLP\New_Installs\Release` directory to the computer where you plan to install the detection server.

3 Run the `ServerJRE.msi` file to display the **Symantec Data Loss Prevention Server JRE Setup** dialog.

4 After you review the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.

5 In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**.

Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.

6 Click **Install** to begin the installation process.

7 Click **Finish** to complete the process.

Installing a detection server

Follow this procedure to install the detection server software on a server computer. After you install the detection server, you migrate previous version data to complete the upgrade process.

Note: The following instructions assume that the `DetectionServer.msi` file has been copied into the `c:\temp` directory on the server computer.

Using the graphical user interface method to install does not generate log information. To generate log information, run the installation using the following command:

```
msiexec /i DetectionServer.msi /L*v c:\detectionserver_install.log
```

You can complete the installation using Silent Mode. Enter values with information specific to your installation for the following:

Table 2-3 Detection server Silent Mode installation parameters

Command	Description
`DATA_DIRECTORY`	Defines where Symantec Data Loss Prevention stores files that are updated while the Enforce Server is running (for example, logs and licenses). The default location is `\ProgramData\Symantec\DataLossPrevention\DetectionServer\`. **Note:** If you do not use the default location, you must indicate a folder name for the data directory. If you set the data directory to the drive root (for example `c:\` or `e:\`) you cannot successfully uninstall the program.
`JRE_DIRECTORY`	Specifies where the JRE resides.

Table 2-3 Detection server Silent Mode installation parameters *(continued)*

Command	Description
FIPS_OPTION	Defines whether to disable (**Disabled**) or enable (**Enabled**) FIPS encryption.
SERVICE_USER_OPTION	Defines whether to create a new service user by entering **NewUser** or using an existing one by entering **ExistingUser**.
SERVICE_USER_USERNAME	Defines a name for the account that is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.”
SERVICE_USER_PASSWORD	Defines the password for the account that is used to manage Symantec Data Loss Prevention services.
UPDATE_USER_USERNAME	Defines a name for the account that is used to manage Symantec Data Loss Prevention update services. The default user name is “SymantecDLPUpdate.”
UPDATE_USER_PASSWORD	Defines the password for the account that is used to manage Symantec Data Loss Prevention update services.
BIND_HOST	Defines the host name or IP address of the detection server.
BIND_PORT	Defines the port on which the detection server should accept connections from the Enforce Server. If you cannot use the default port (8100), you can enter any port higher than port 1024, in the range of 1024–65535.

The following is an example of what the completed command might look like. The command you use differs based on your implementation requirements. Using the following command as-is may cause the installation to fail.

```
msiexec /i DetectionServer.msi /qn /norestart /Lv DetectionServer.log
INSTALLATION_DIRECTORY="C:\Program Files\Symantec\Data Loss Prevention"
DATA_DIRECTORY="C:\ProgramData\Symantec\Data Loss Prevention\Detection Server"
JRE_DIRECTORY="C:\Program Files\Symantec\Data Loss Prevention\Server JRE\1.8.0_181"
FIPS_OPTION=Disabled
SERVICE_USER_OPTION=ExistingUser
SERVICE_USER_USERNAME=SymantecDLP
SERVICE_USER_PASSWORD=Password
UPDATE_USER_USERNAME=SymantecDLPUpdate
UPDATE_USER_PASSWORD=Password
DETECTION_COMMUNICATION_DEFAULT_CERTIFICATES=enabled
BIND_HOST=xxx.xxx.xxx.xxx
BIND_PORT=8100
```

To install a detection server

1 Ensure that installation preparations are complete.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 9.

2 Log on as Administrator to the computer on which you plan to install the detection server.

3 If you are installing a Network Monitor detection server, install WinPcap on the server computer. Follow these steps:

- On the Internet, go to the following URL: http://www.winpcap.org/archive/
- Download WinPcap to a local drive.
- Double-click on the `WinPcap.exe` and follow the on-screen installation instructions.

4 Copy the detection server installer (`DetectionServer.msi`) from the Enforce Server to a local directory on the detection server.

`DetectionServer.msi` 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.

Note: Using the graphical user interface method to install does not generate log information. To generate log information, run the installation using the following command:

```
msiexec /i DetectionServer.msi /L*v c:\detectionserver_install.log
```

---

5 Click **Start > Run > Browse** to navigate to the folder where you copied the `DetectionServer.msi` file.

6 Double-click `DetectionServer.msi` to execute the file, and click **OK**.

The installer files unpack, and the **Welcome** panel of the Installation Wizard displays.

7 Click **Next**.

The **End-User License Agreement** panel displays.

8 After reviewing the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.

9 In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**.

For example: `c:\Program Files\Symantec\DataLossPrevention\`

Symantec recommends that you use the default destination directory. However, you can click Browse to navigate to a different installation location instead.

Note: Directory names, IP addresses, and port numbers created or specified during the installation process must be entered in standard 7-bit ASCII characters only. Extended (hi-ASCII) and double-byte characters are not supported.

---

10 In the **JRE Directory** panel, accept the default JRE location (or click **Browse** to locate it), and click **Next**.

11 In the **FIPS Cryptography Mode** panel, select whether to disable or enable FIPS encryption.

12 In the **Service User** panel, select one of the following options, then click **Next**.

- **New Users**: Select this option to create the Symantec Data Loss Prevention system account user name and password and confirm the password. This account is used to manage Symantec Data Loss Prevention services. The default user name is "SymantecDLP." New service user accounts are local accounts.

  Note: To use the RMS detection feature, you must enable it after installing the detection server.

  The password you enter for the System Account must conform to the password policy of the server. For example, the server may require all passwords to include special characters.

- **Existing Users**: Select this option to use an existing local or domain user account. Enter a domain service user name and password if you plan to manage the detection server with a domain user. If you want to use the RMS detection feature, ensure that the domain user that you enter has access to the RMS AD system (and is a member of the selected AD RMS Super Users group) or the Azure RMS system.

Click **Next**.

13 (Optional) If you opted to create a new service user, enter the new account name and password. Confirm the password, then click **Next**.

14 (Optional) If you opted to use an existing local or domain user account, enter the account name and password. The user name for a domain users must be in ***DOMAIN\username*** format.

15 In the **Update User** panel, enter the account name and password. The default user name is "SymantecDLPUpdate."

This account is used to manage updates sent to the detection server.

16 In the **Server Bindings** panel, enter the following settings:

- **Host**. Enter the host name or IP address of the detection server.
- **Port**. Accept the default port number (8100) on which the detection server should accept connections from the Enforce Server. If you cannot use the default port, you can change it to any port higher than port 1024, in the range of 1024–65535.

17 Click **Install** to begin the installation process.

The **Installing** panel appears, and displays a progress bar. After a successful installation, the **Completing** panel appears.

18 Restart any antivirus, pop-up blocker, or other protection software that you disabled before starting the detection server installation process.

19 Verify that the detection server is properly installed.

Running the Migration Utility on a detection server

You can complete the migration using Silent Mode. Use the following command:

```
DetectionServerMigrationUtility
-silent
-sourceInstallation="previous active version path"
```

Where *previous active version path* represents where the previous version is installed (for example, `C:\SymantecDLP)`.

To migrate data from a previous detection server version to version 15.5

1 Use the command prompt to navigate to the following directory:

```
C:\Program
Files\Symantec\DataLossPrevention\DetectionServer\15.5\Protect\Migrator
```

2 Run the Migration Utility: `DetectionServerMigrationUtility`.

3 Select the Symantec Data Loss Prevention version to migrate and press **Enter**.

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.

Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.5 installation. If you uninstall the previous version, the service_user is removed.

---

4 If the migration fails, review the detection server migration logs in `MigrationUtility.log` located at `C:\ProgramData\Symantec\DataLossPrevention\DetectionServer\15.5\logs\debug`.

Migrating previous version data to a new single-tier installation

After you install the version 15.5 single-tier system, you use the Migration Utility to migrate data to the new instance. Before you run the Migration Utility, run the Update Readiness tool to confirm that the database is ready for migration.

See "Checking the database update readiness" on page 13.

To upgrade a single-tier installation to the latest version

1 Install the Java Runtime Environment on the Enforce Server.

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

See "Installing the Java Runtime Environment on the Enforce Server" on page 31.

2 Run the Update Readiness tool.

Running the tool identifies potential issues with the database.

See "Creating the Update Readiness tool database account" on page 15.

3 Install the version 15.5 single-tier system.

You install the single-tier system on the same computer where the previous version is running.

See "Installing a single-tier server" on page 45.

4 Migrate the previous version to the version 15.5 single-tier installation.

See "Running the Migration Utility on single-tier installation" on page 50.

Installing the Java Runtime Environment for a single-tier installation

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

To install the JRE

1. Copy `ServerJRE.msi` to the computer where you plan to install the single-tier system.
2. Log on (or remote logon) as Administrator to the computer where you plan to install the single-tier system.
3. Unzip the file contents (for example, unzip to `c:\temp`).
4. Run the `ServerJRE.msi` file to display the **Symantec Data Loss Prevention Server JRE Setup** dialog.
5. After you review the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.
6. In the **Destination Folder** panel, accept the default destination directory, or enter an alternate directory, and click **Next**.

   Symantec recommends that you use the default destination directory. References to the "installation directory" in Symantec Data Loss Prevention documentation are to this default location.
7. Click **Install** to begin the installation process.
8. Click **Finish** to complete the process.

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.

The following instructions assume that the `SingleTierServer.msi` file, license file, and solution pack file have been copied into the `c:\temp` directory on the Enforce Server.

Using the graphical user interface method to install does not generate log information. To generate log information, run the installation using the following command:

```
msiexec /i SingleTierServer.msi /L*v c:\enf_data\enforce_install.log.
```

After you complete the Single Tier installation, you can find the installation log file at `c:\enf_data`.

You can complete the installation using Silent Mode. Enter values with information specific to your installation for the following:

Table 2-4 Single-tier server silent mode installation parameters

Command	Description
INSTALLATION_DIRECTORY	Specifies where the Enforce Server is installed. The default location is `C:\Program Files\Symantec\DataLossPrevention`.
DATA_DIRECTORY	Defines where Symantec Data Loss Prevention stores files that are updated while the Enforce Server is running (for example, logs and licenses). The default location is `C:\ProgramData\Symantec\DataLossPrevention`. **Note:** If you do not use the default location, you must indicate a folder name for the data directory. If you set the data directory to the drive root (for example `c:\` or `e:\`) you cannot successfully uninstall the program.
JRE_DIRECTORY	Specifies where the JRE resides.
FIPS_OPTION	Defines whether to disable (**Disabled**) or enable (**Enabled**) FIPS encryption.
SERVICE_USER_OPTION	Defines whether to create a new service user by entering **NewUser** or using an existing one by entering **ExistingUser**.
SERVICE_USER_USERNAME	Defines a name for the account that is used to manage Symantec Data Loss Prevention services. The default user name is “SymantecDLP.”
SERVICE_USER_PASSWORD	Defines the password for the account that is used to manage Symantec Data Loss Prevention services.
ORACLE_HOME	Defines the Oracle Home Directory. For example, use `c:\oracle\product\12.2.0.1\db_1` to define the home directory if you use the Oracle 12.2.0.1 database.
ORACLE_HOST	Defines the IP address of the Oracle server computer.
ORACLE_PORT	Defines the Oracle listener port (typically 1521).
ORACLE_USERNAME	Defines the Symantec Data Loss Prevention database user name.

Table 2-4 Single-tier server silent mode installation parameters *(continued)*

Command	Description
ORACLE_PASSWORD	Defines the Symantec Data Loss Prevention database password.
ORACLE_SERVICE_NAME	Defines the database SERVICE_NAME (typically “protect”).
EXTERNAL_STORAGE_OPTION	Defines whether incident attachments are stored in the database (**Database**) or in external storage (**ExternalStorage**).
EXTERNAL_STORAGE_DIRECTORY	Defines the path where you plan to store incident attachments.
UPDATE_USER_USERNAME	Defines a name for the account that is used to manage Symantec Data Loss Prevention update services. The default user name is “SymantecDLPUpdate.”
UPDATE_USER_PASSWORD	Defines the password for the account that is used to manage Symantec Data Loss Prevention update services.
BIND_PORT	Defines the port on which the server should accept connections from the Enforce Server. If you cannot use the default port (8100), you can enter any port higher than port 1024, in the range of 1024–65535.
ADDITIONAL_LOCALE	Defines an additional locale for use by individual users.
ENFORCE_ADMINISTRATOR_PASSWORD	Defines the Enforce Server administration console password. This parameter is required during the migration.

The following is an example of what the completed command might look like. The command you use differs based on your implementation requirements. Using the following command as-is may cause the installation to fail.

```
msiexec /i SingleTierServer.msi /qn /norestart /L*v SingleTier.log
INSTALLATION_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention"
DATA_DIRECTORY="C:\ProgramData\Symantec\DataLossPrevention"
JRE_DIRECTORY="C:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181"
FIPS_OPTION=Disabled
SERVICE_USER_OPTION=ExistingUser
```

```
SERVICE_USER_USERNAME=SymantecDLP
SERVICE_USER_PASSWORD=Symantec1
ORACLE_HOME="C:\oracle\product\12.2.0.1\db_1"
ORACLE_HOST=xxx.xxx.xxx.xxx
ORACLE_USERNAME=protect
ORACLE_PASSWORD=Password
ORACLE_SERVICE_NAME=protect
EXTERNAL_STORAGE_OPTION=database
UPDATE_USER_USERNAME=SymantecDLPUpdate
UPDATE_USER_PASSWORD=Password
ENFORCE_ADMINISTRATOR_PASSWORD=Password
```

To install the single-tier server

1. Log on (or remote logon) as Administrator to the computer that is intended for the Symantec Data Loss Prevention single-tier installation.
2. Install WinPcap on the system before you install the detection server. Follow these steps:
   - On the Internet, go to the following URL: http://www.winpcap.org/archive/
   - Download WinPcap to a local drive.
   - Double-click on the `WinPcap.exe` and follow the on-screen installation instructions.
3. Copy the Symantec Data Loss Prevention installer (`SingleTierServer.msi`) from *`DLPDownloadHome`* to a local directory on the computer where you plan to install the single-tier system.
4. Click **Start > Run > Browse** to navigate to the folder where you copied the `SingleTierServer.msi` file.
5. Double-click `SingleTierServer.msi` to execute the file, and click **OK.**
6. The installer files unpack, and a welcome notice appears. Click **Next**.
7. In the **End-User License Agreement** panel, select **I accept the terms in the License Agreement**, and click **Next**.
8. In the **Destination Folder** panel, accept the Symantec Data Loss Prevention default destination directory and click **Next**.

   ```
   c:\Program Files\Symantec\DataLossPrevention
   ```

   Symantec recommends that you use the default destination directory. However, you can click **Browse** to navigate to a different installation location instead.

   Directory names, account names, passwords, IP addresses, and port numbers created or specified during the installation process must be entered in standard 7-bit ASCII characters only. Extended (hi-ASCII) and double-byte characters are not supported.

9 In the **JRE Directory** panel, accept the default JRE location (or click **Browse** to locate it), and click **Next**.

10 In the **FIPS Cryptography Mode** panel, select whether to disable or enable FIPS encryption.

11 In the **Service User** panel, select one of the following options, then click **Next**.

- **New Users**: Select this option to create the Symantec Data Loss Prevention system account user name and password and confirm the password. This account is used to manage Symantec Data Loss Prevention services. The default user name is "SymantecDLP." New service user accounts are local accounts.

  Note: To use the RMS detection feature, you must enable it after installing the detection server.

  The password you enter for the System Account must conform to the password policy of the server. For example, the server may require all passwords to include special characters.

- **Existing Users**: Select this option to use an existing local or domain user account. Enter a domain service user name and password if you plan to manage the detection server with a domain user. If you want to use the RMS detection feature, ensure that the domain user that you enter has access to the RMS AD system (and is a member of the selected AD RMS Super Users group) or the Azure RMS system.

12 Click **Next**.

13 (Optional) If you opted to create a new service user, enter the new account name and password. Confirm the password, then click **Next**.

14 (Optional) If you opted to use an existing local or domain user account, enter the account name and password. The user name must be in ***DOMAIN**username*** format.

15 In the **Update User** panel, enter the account name and password. The default user name is "SymantecDLPUpdate."

This account is used to manage updates sent to the detection server.

16 In the **Oracle Database Server Information** panel, enter the **Oracle Database Server** host name or IP address and the **Oracle Listener Port**.

Default values should already be present for these fields. Since this is a single-tier installation with the Oracle database on this same system, **127.0.0.1** is the correct value for **Oracle Database Server Information** and **1521** is the correct value for the **Oracle Listener Port**.

Click **Next**.

17 Click **Next**.

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

18 If you choose to store your incident attachments externally, check the **Enable external storage for incident attachments** box and enter the path or browse to your external storage directory.

19 In the **Additional Locale** panel, select an alternate locale, or accept the default of None, and click **Next**.

Locale controls the format of numbers and dates, and how lists and reports are alphabetically sorted. If you accept the default choice of None, English is the locale for this Symantec Data Loss Prevention installation. If you choose an alternate locale, that locale becomes the default for this installation, but individual users can select English as a locale for their use.

See the *Symantec Data Loss Prevention Administration Guide* for more information on locales.

20 In the **Server Bindings** panel, enter the following settings:

- **Host**. Enter the host name or IP address of the detection server.
- **Port**. Accept the default port number (8100) on which the detection server should accept connections from the Enforce Server. If you cannot use the default port, you can change it to any port higher than port 1024, in the range of 1024–65535.

21 Click **Install** to begin the installation process.

The **Installing** panel appears, and displays a progress bar. After a successful installation, the **Completing** panel displays.

22 Verify the Symantec Data Loss Prevention single-tier installation.

23 If you have not done so already, run the Upgrade 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.

24 Create the Enforce Reinstallation Resources file. This file contains the unique `CryptoMasterKey.properties` file and keystore files for your Symantec Data Loss Prevention deployment.

See “Creating the Enforce Reinstallation Resources file” on page 92.

Running the Migration Utility on single-tier installation

After you install the 15.5 single-tier system, you can migrate data using the Migration Utility.

See “Checking the database update readiness” on page 13.

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

See "To migrate data from a previous single-tier installation version to version 15.5 using interactive mode" on page 51.

To migrate data from a previous single-tier installation version to version 15.5 using Silent Mode

- Run the following command in an elevated command prompt:

  ```
  SingleTierServerMigrationUtility
  -silent
  -sourceInstallation="previous version path"
  ```

  Where *previous version path* represents where the previous, active version is installed (for example, `C:\SymantecDLP`).

To migrate data from a previous single-tier installation version to version 15.5 using interactive mode

1. Log on (or remote logon) as Administrator to the Single Tier Server system where you intend to run the Migration Utility.
2. Use the command prompt to navigate to the following directory:

   ```
   C:\Program
   Files\Symantec\DataLossPrevention\SingleTierServer\15.5\Protect\Migrator
   ```

3. Run the Migration Utility: `SingleTierServerMigrationUtility`.
4. Select the active Symantec Data Loss Prevention version to migrate and press **Enter**.

   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.

   Note: The previous version is still installed but all services are in a disabled state. You can restart these services if you re-used the service_user during the version 15.5 installation. If you uninstall the previous version, the service_user is removed.

   ---

5. If migration fails, review the Enforce Server migration logs in the `MigrationUtility.log` located at `C:\ProgramData\Symantec\DataLossPrevention\SingleTierServer\15.5\logs\debug`.

Verifying that the Enforce Server and the detection servers are running

Verify that the Enforce Server is running.

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

See "About Symantec Data Loss Prevention services" on page 84.

To ensure that the detection servers are running

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

See "Upgrading Symantec Data Loss Prevention" on page 28.

Applying the updated configuration to Endpoint Prevent servers

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

To apply the updated configuration to Endpoint Prevent servers

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

Upgrading your scanners

If you have any version 14.0 or earlier scanners, you should upgrade them to Symantec Data Loss Prevention version 15.5 scanners. To upgrade a scanner, remove the older software and then install the Symantec Data Loss Prevention 15.5 scanner.

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

See "Symantec Data Loss Prevention upgrade phases" on page 10.

Upgrading Endpoint Prevent group directory connections

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

See the *Symantec Data Loss Prevention System Administration Guide* for information about creating group directory connections and scheduling directory server indexing: http://www.symantec.com/docs/DOC9261

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* at the Symantec Support Center at http://www.symantec.com/docs/DOC9261.

Chapter 3

Upgrading Symantec DLP Agents

This chapter includes the following topics:

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 15.5 Endpoint Server. Endpoint Servers are backward-compatible with a DLP Agent for one full release. For example, a version 15.5 Endpoint Server and a version 14.x DLP Agent are compatible.

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

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

The following table provides a general overview of the upgrade process:

Table 3-1 Upgrade process for Symantec DLP Agents

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 you use to upgrade Windows agents and a PKG file you use to upgrade the Mac agents. See "About secure communications between DLP Agents and Endpoint Servers" on page 55.
2	Bundle the Mac agent installation files if you plan to upgrade Mac agents.	See "Process to upgrade the DLP Agent on Mac" on page 66.
3	Install the upgrade package on endpoints.	Choose one of the following upgrade methods: ■ Upgrade the DLP Agent by using silent upgrades. See "Upgrading the Windows agent silently" on page 64. See "Upgrading DLP Agents on Mac endpoints silently" on page 70. ■ Upgrade the DLP Agent manually. See "Upgrading the Windows agent manually" on page 63. See "Upgrading the DLP Agent for Mac manually" on page 69.

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.

See "Working with endpoint certificates" on page 62.

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

You use the Enforce Server administration console to generate the agent certificate and keys. The system packages the agent certificates and keys with the agent installer for deployment of DLP Agents.

See "Generating agent installation packages" on page 56.

Generating agent installation packages

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

See "About secure communications between DLP Agents and Endpoint Servers" on page 55.

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

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

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

- Confirm that the agent installers are copied to the Enforce Server local file system.
  See "Downloading and extracting the upgrade software" on page 30.
- Confirm that the Enforce Server has at least 3 GB of free space. The packaging process fails if the Enforce Server has less than 3 GB of free space.

Table 3-2 provides instructions for generating agent installation packages. The instructions assume that you have deployed an Endpoint Server.

Table 3-2 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.

Table 3-2 Generating the agent installation package *(continued)*

Step	Action	Description
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 15.5 64-bit installation file while selecting **Version 15.1 and later** in the list is unsupported. Selecting mis-matched versions prevents agents from installing on endpoints. If you plan to package an ICT Client and ICE Utility with the DLP agent, you must select **Version 15.1 and later**.
3	Select one or more DLP Agent installation files.	Browse to the folder on the Enforce Server where you copied the agent installer files: **Windows 64-bit**: `AgentInstallers-x64_15_5.zip` **Windows 32-bit**: `AgentInstallers-x86_15_5.zip` **Mac 64-bit**: `AgentInstallers-x86_64_15.5.zip`
4	Enter the server host name.	Typically you enter the common name (CN) of the Endpoint Server host, or you can enter the IP address of the server. Be consistent with the type of identifier you use (CN or IP). If you used the CN for the Endpoint Server when deploying it, use the same CN for the agent package. If you used an IP address to identify the Endpoint Server, use the same IP address for the agent package. Alternatively, you can enter the CN or IP address of a load balancer server.
5	Enter the port number for the server.	The default port is 10443. Typically you do not need to change the default port unless it is already in use or intended for use by another process on the server host.

Table 3-2 Generating the agent installation package *(continued)*

Step	Action	Description
6	Add additional servers (optional).	Click the plus sign to add additional servers for failover. **Note:** Symantec Data Loss Prevention allots 2048 characters for Endpoint Server names. This allotment includes the characters that are used for the Endpoint Server name, port numbers, and semicolons to delimit each server. The first server that is listed is the primary; additional servers are secondary and provide backup if the primary is down.
7	Enter the Endpoint tools password.	A password is required to use the Endpoint tools to administer DLP Agents. The Endpoint tools password is case-sensitive. The password is encrypted and stored in a file on the Enforce Server. You should store this password in a secure format of your own so that it can be retrieved if forgotten. After installing agents, you can change the password on the **Agent Password Management** screen.
8	Re-enter the Endpoint tools password.	The system validates that the passwords match and displays a message if they do not.
9	Enter the target directory for the agent installation (Windows only).	The default installation directory for Windows 32- and 64-bit agents is `%PROGRAMFILES%\Manufacturer\Endpoint Agent`. Change the default path if you want to install the Windows agent to a different location on the endpoint host. You can only install the DLP Agent to an ASCII directory using English characters. Using non-English characters can prevent the DLP Agent from starting and from monitoring data in some scenarios. **Note:** Include the drive letter if you plan to change the default directory. For example, use `C:\Endpoint Agent`. Not including a drive letter causes the agent installation to fail. The target directory for the Mac agent is set by default.

Table 3-2 Generating the agent installation package *(continued)*

Step	Action	Description
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. For information on uninstalling Mac agents, refer to the topic "Removing a DLP Agent from a Mac endpoint" in the *Symantec Data Loss Prevention Installation Guide*. After installing agents, you can change the password on the **Agent Password Management** screen.
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 the ICT Client with the agent package. Enter the License and ICT Web Service URL. Go to the Information Centric Tagging Administration Console to gather information for the following fields: ■ **License** After the ICT admin installs the ICT server and uploads a license file on the Server Keys tab, a server public key displays. Enter that key in the **License** field. ■ **ICT Web Service URL** The ICT admin defines this URL on the **Encryption** tab, in the **URL of Rights Template Manager Web Services** field. Enter that URL in the **ICT Web Service URL** field. For more information about these two fields, see the *Symantec Information Centric Tagging Deployment Guide*: http://www.symantec.com/docs/DOC11257

Table 3-2 Generating the agent installation package *(continued)*

Step	Action	Description
13	(Optional) Select **Install the Symantec ICE Utility**.	Select this option to package the ICE Utility with the agent package. For more information about the ICE Utility, see the *Symantec Information Centric Encryption Deployment Guide*: http://www.symantec.com/docs/DOC9707 **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. 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.

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 23.
		See "Agent installation package contents" on page 60.

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.

See "Generating agent installation packages" on page 56.

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

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

File name	Description
`AgentInstall-x86_15_5.msi`	Windows agent installer
`endoint_cert.pem`	Agent certificate and encryption keys See "Working with endpoint certificates" on page 62.
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`ICSEndpoint-x64_15_5.exe`	Use to install the ICT Client and ICE Utility.
`install_agent.bat`	Use to install the DLP Agent, ICT Client, and ICE Utility silently.
`rw-config.ini`	Use to install the ICT Client silently. For additional details on this file, refer to the *Symantec Information Centric Tagging Deployment Guide*:: http://www.symantec.com/docs/DOC11257
`upgrade_agent.bat`	Use to upgrade the DLP Agent, ICT Client, and ICE Utility silently.

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

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

File	Description
`AgentInstall_15_5.pkg`	Mac DLP Agent installer
`AgentInstall.plist`	Mac DLP Agent installation properties configuration file
`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).

Table 3-4 `AgentInstaller_Mac64.zip` installation package contents *(continued)*

File	Description
`endoint_cert.pem`	Agent certificate and encryption keys See "Working with endpoint certificates" on page 62.
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`ICEReader_Managed_15_5.pkg`	ICE client installer
`install_agent.sh`	Use to install the DLP Agent and the ICE Utility.
`Install_Readme.rtf`	Provides commands for packaging and installing the agent See "Process to upgrade the DLP Agent on Mac" on page 66.

Working with endpoint certificates

Symantec Data Loss Prevention automatically generates the public certificates and the keys needed for authentication and secure communications between DLP Agents and Endpoint Server. The public certificates and keys are securely stored in the Enforce Server database.

See "About secure communications between DLP Agents and Endpoint Servers" on page 55.

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

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

See "Generating agent installation packages" on page 56.

Process to upgrade the DLP Agent on Windows

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

Before you upgrade DLP Agents on Windows endpoints, confirm that you have completed prerequisite steps. See "About Symantec Data Loss Prevention Agent upgrades" on page 54.

Table 3-5 Process to upgrade agents on Windows endpoints

Step	Action	Description
1	Prepare endpoints that have Safe Mode monitoring enabled.	See "Upgrading previous version DLP Agents with Windows Safe Mode monitoring enabled" on page 63.
2	Upgrade the agent. Upgrade an agent manually. You can upgrade an agent manually when you want to test the configuration. Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time.	See "Upgrading the Windows agent manually" on page 63. See "Upgrading the Windows agent silently" on page 64.

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 15.5, you must delete the registry entries for the TDI drivers before you upgrade the agents.

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

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

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

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

Upgrading the Windows agent manually

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

These steps assume that you have generated the agent installation package. See "Generating agent installation packages" on page 56.

To install the DLP Agent manually

1 Run the DLP Agent upgrade batch file.

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

2 Confirm that the agent is running.

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

Upgrading the Windows agent silently

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

Note: These steps assume that you have generated the agent installation package. See "Generating agent installation packages" on page 56.

To perform a silent upgrade

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

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

2 Specify the `upgrade_agent.bat` installation properties.

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

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

The following table outlines each command and what it does.

`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 (the services should appear in the list).

See "About Symantec Data Loss Prevention Agent upgrades" on page 54.

Process to upgrade the DLP Agent on Mac

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

Before you upgrade DLP Agents on Mac endpoints, confirm that you have completed prerequisite steps. See "About Symantec Data Loss Prevention Agent upgrades" on page 54.

Table 3-6 Process to install 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.	See "Packaging Mac agent upgrade files" on page 67.
2	Upgrade the agent. Upgrade an agent manually. You can upgrade an agent manually when you want to test the configuration. Upgrade the agents using your SMS. You upgrade agents using this method to upgrade many agents at one time.	See "Upgrading the DLP Agent for Mac manually" on page 69. See "Upgrading DLP Agents on Mac endpoints silently" on page 70.
3	Confirm that the Mac agent service is running.	See "Confirming that the Mac agent is running" on page 71.
4	(Optional) Review the upgraded Mac agent components. These components include the drivers that prevent tampering and keep the agent running.	See "What gets upgraded for DLP Agents on Mac endpoints" on page 71.

Packaging Mac agent upgrade files

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

The following steps assume that you have generated the agent installation package and completed all prerequisites. See “About secure communications between DLP Agents and Endpoint Servers” on page 55.

To package the Mac agent upgrade files:

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

See "Agent installation package contents" on page 60.

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

`$ cd /tmp/MacInstaller`	Defines the path where the Mac agent upgrade files reside.
`$ ./create_package`	Calls the create_package tool.
`-i <com.company.xyz>`	(Optional) Includes a custom package identifier. You can register the DLP Agent installer receipt data with a custom package identifier. Replace `<com.company.xyz>` with information specific to your deployment.
`-t ./Tools`	(Optional) Calls the create_package tool to bundle the agent tools. See "About optional installation and maintenance tools" on page 69.

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

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

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

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

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

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

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

See "Upgrading DLP Agents on Mac endpoints silently" on page 70.

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_15.5_Agent_Mac-IN.zip` file.

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

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

See "Packaging Mac agent upgrade files" on page 67.

Table 3-7 lists the available tools.

Table 3-7 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

Table 3-8 provides steps for upgrading the DLP Agent for Mac manually.

Normally you perform a manual installation or upgrade when you want to test the agent installation package. If you do not plan to test the agent installation package, you install Mac agents using an SMS. See "Upgrading DLP Agents on Mac endpoints silently" on page 70.

Note: The following steps assume that you have generated the agent installation package and completed all prerequisites. See "About secure communications between DLP Agents and Endpoint Servers" on page 55.

Table 3-8 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.	For example, unzip the file to `/tmp/MacInstaller`.

Table 3-8 Instructions for upgrading the DLP Agent on a Mac endpoint *(continued)*

Step	Action	Description
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_5.pkg -target /` Replace `/tmp/MacInstaller` with the path where you unzipped the agent installation package.
3	Verify the Mac agent upgrade.	To verify the Mac agent installation, open the Activity Monitor and search for the **edpa** process. It should be up and running. The Activity Monitor displays processes being run by logged in user and edpa runs as root. Select **View All Processes** to view **edpa** if you are not logged in as root user. You can also confirm that agent was installed to the default directory: `/Library/Manufacturer/Endpoint Agent`.
4	(Optional) Troubleshoot the upgrade.	If you experience upgrade issues, use the Console application to check the log messages. Review the Mac Agent installer logs at `/var/log/install.log`. In addition, you can rerun the installer with `-dumplog` option to create detailed installation logs. For example, use the command `sudo installer -pkg /tmp/AgentInstall/AgentInstall_15_5.pkg -target / -dumplog`. Replace `/tmp/MacInstaller` with the path where you unzipped the agent installation package.
5	(Optional) Review information about the Mac agent installation.	See "What gets upgraded for DLP Agents on Mac endpoints" on page 71.

Upgrading DLP Agents on Mac endpoints silently

You can use a silent upgrade process by using systems management software (SMS) to upgrade DLP Agents. You must always upgrade the agent installation package from a local directory. If you do not upgrade from a local directory, some functions of the DLP Agent are disabled.

These steps assume that you have generated the agent installation package and packaged the Mac agent installation files.

See "Generating agent installation packages" on page 56.

See "Packaging Mac agent upgrade files" on page 67.

To perform an unattended upgrade

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

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

Confirming that the Mac agent is running

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

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

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

See "What gets upgraded for DLP Agents on Mac endpoints" on page 71.

What gets upgraded for DLP Agents on Mac endpoints

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

Table 3-9 Mac agent components

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/`.

Table 3-9 Mac agent components *(continued)*

Component	Description
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).

Chapter 4

Post-upgrade tasks

This chapter includes the following topics:

Performing post-upgrade tasks

You must perform certain tasks after you finish upgrading.

See “Verifying Symantec Data Loss Prevention operations” on page 73.

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

Verifying Symantec Data Loss Prevention operations

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

To verify Symantec Data Loss Prevention operations

1. Log on to the Enforce Server administration console as Administrator.
2. Log out of the Enforce Server administration console and then log on as a user other than Administrator.
3. Go to the **System Overview** screen and recycle the current version detection servers to verify that they are connected.

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

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

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

7 Network Discover provides incremental scanning for certain target types. After you upgrade Symantec Data Loss Prevention, verify that incremental scanning is configured for valid targets. See the *Symantec Data Loss Prevention System Administration Guide* for information about configuring incremental scans.

8 If you have deployed any Lookup plug-ins, go to the **System** > **Lookup Plugins** screen and verify that the plug-in appears in the list of plug-ins and is configured correctly.

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

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

Enabling Microsoft Rights Management file monitoring

Symantec Data Loss Prevention can detect files that are encrypted using Microsoft Rights Management (RMS) administered by Azure or Active Directory (AD). Before you enable Microsoft Rights Management file monitoring, confirm that prerequisites for the RMS environment and detection server have been completed. See "Preparing your environment for Microsoft Rights Management file monitoring" on page 26.

Enable RMS decryption for Azure

To enable Azure RMS, complete the following on each detection server:

1 Run the `Enable-Plugin.ps1` (located in `C:\Program Files\Symantec\DataLossPrevention\ContentExtractionService\15.5\Plugins\Protect\plugins\contentextraction\MicrosoftRightsManagementPlugin` on the Enforce Server) from the local machine user (protect user). For example, run:

```
powershell -Executionpolicy Remotesigned -File Enable-Plugin.ps1
```

2 Run the Configuration Creator utility (`ConfigurationCreator.exe`) to add the service user. Run the utility as the protect user. Enter your Azure RMS licensing information when running the script. For example, run:

```
C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\
plugins\contentextraction\
```

```
MicrosoftRightsManagementPlugin\ConfigurationCreator.exe
Do you want to configure ADAL authentication [y/n]: n
Do you want to configure symmetric key authentication [y/n]: y
Enter your symmetric key (base-64): [user's Azure RMS symmetric key]
Enter your app principal ID: [user's Azure RMS app principal ID]
Enter your BPOS tenant ID: [user's Azure RMS BPOS tenant ID]
```

After running this script, the following files are created in the `MicrosoftRightsManagementPlugin` folder at `C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\plugins\contentextraction\`:

- `rightsManagementConfiguration`
- `rightsManagementConfigurationProtection`

3. Restart each detection server on the Enforce Server administration console to complete the process to enable RMS monitoring.
4. Confirm that Symantec Data Loss Prevention is monitoring RMS content by reviewing the `ContentExtractionHost_FileReader.log` file (located at `\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\Logs\debug`) and confirming the `MicrosoftRightsManagementPlugin` item has been initialized.

Enable RMS decryption for AD

To enable AD RMS, complete the following on each detection server:

1. Run the `Enable-Plugin.ps1` (located in `C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\bin` on the Enforce Server). For example, run:

```
powershell -Executionpolicy Remotesigned
-File Enable-Plugin.ps1
```

2. Restart each detection server on the Enforce Server administration console to complete the process to enable RMS monitoring.
3. Confirm that Symantec Data Loss Prevention is monitoring RMS content by reviewing the `ContentExtractionHost_FileReader.log` file (located at `\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\Logs\debug`) and confirming the `MicrosoftRightsManagementPlugin` item has been initialized.

Migrating plug-ins

During the upgrade process, the Migration Utility moves plug-ins from the previous version system to the new system location: `\Program`

Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\plugins. Specifically, the following plug-ins are migrated:

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

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

To migrate remaining plug-ins

1. Locate plug-ins you plan to move.

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

2. Copy plug-ins to the following locations on the new version system:
   - Enforce Server:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\plugins
   - Detection server: \Program Files\Symantec\DataLossPrevention\DetectionServer\15.5\Protect\plugins

About securing communications between the Enforce Server and the database

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

You must upgrade Symantec Data Loss Prevention before you secure communications between the Enforce Server and the database using TLS. The Symantec Data Loss Prevention upgrade cannot communicate over TLS. See "Upgrading Symantec Data Loss Prevention" on page 28.

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

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

Step	Action	More info
1	Generate the self-signed certificates using the orapki command-line utility that is provided with the Oracle database.	See "About orapki command line options" on page 77. See "Using orapki to generate the server certificate on the Oracle database" on page 78.
2	Configure the JDBC driver on the Enforce Server to use the TLS connection and port.	See "Configuring communication on the Enforce Server" on page 79.
3	Configure the server certificate on the Enforce Server.	See "Configuring the server certificate on the Enforce Server" on page 81.

About orapki command line options

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

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

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

Table 4-2 Orapki utility examples

Command and options	Description
`orapki wallet create -wallet c:\oracle\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 c:\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 c:\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.

Table 4-2 Orapki utility examples *(continued)*

Command and options	Description
`orapki wallet export -wallet c:\oracle\wallet\server_wallet -dn "CN=oracleserver" -cert c:\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 `c:\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.

To generate certificates

1. Shut down all Oracle services if they are running in Windows Services.

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

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

   ```
   cd c:\oracle
   ```

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

   ```
   mkdir wallet
   ```

   ```
   cd wallet
   ```

4. Create a wallet on the Oracle server with auto login enabled by running the following command in the `c:\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`

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

```
orapki wallet add -wallet c:\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.

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

```
orapki wallet display -wallet c:\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
```

7 Export the certificate by running the following command:

```
orapki wallet export -wallet c:\oracle\wallet\server_wallet -dn
"CN=oracleserver" -cert c:\oracle\wallet\server_wallet\cert.txt
```

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

```
c:\oracle\wallet\server_wallet
```

Configuring communication on the Enforce Server

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

To configure the JDBC driver on the Enforce Server

1 Back up the `listener.ora` file before you update it.

The file is located at `%ORACLE_HOME%\network\admin`.

2 Stop the listener by running the following command:

```
lsnrctl stop
```

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

3 Open the `listener.ora` file.

4 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))
       )
   )
```

5 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 =
c:\oracle\wallet\server_wallet)))
```

6 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.

7 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 =
c:\oracle\wallet\server_wallet)))
```

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

9 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))
```

10 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**.

11 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:

```
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.

To configure the server certificate on the Enforce Server

1 Locate the `jdbc.properties` file located at `C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\protect\config`.

2 Modify the following communication port and connection information:

- Update the **jdbc.dbalias.oracle-thin** line to use *TCPS*.
- Change the port number to *2484*.

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

```
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"))
```

3 Add the certificate to the `cacerts` file that is located on the Enforce Server by completing the following steps:

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

a Copy the `cert.txt` file to `c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181\lib\security`.

See "Using orapki to generate the server certificate on the Oracle database" on page 78.

b Change the directory by running the following command:

```
cd c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181\lib\security
```

c Insert the certificate into the `cacerts` file by running the following command as an administrator:

```
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 c:\Program Files\Symantec\DataLossPrevention\ServerJRE\1.8.0_181\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

See "About securing communications between the Enforce Server and the database" on page 76.

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

You can find the latest version of the *Symantec Data Loss Prevention Administration Guide* at the following link to the Symantec Support Center article: http://www.symantec.com/docs/DOC9261.

Chapter 5

Starting and stopping Symantec Data Loss Prevention services

This chapter includes the following topics:

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 5-1 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. 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. See "To increase memory for the Symantec DLP Manager service" on page 85.
Symantec DLP Detection Server Controller	Controls the detection servers.
Symantec DLP Notifier	Provides the database notifications.
Symantec DLP Incident Persister	Writes the incidents to the database.

To increase memory for the Symantec DLP Manager service

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

You can find this configuration file in one of the following locations:

- Windows: `\Program Files\Symantec\DataLossPrevention\EnforceServer\Services`
- Linux: `/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.

See "About starting and stopping services on Windows" on page 85.

About starting and stopping services on Windows

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

- See "Starting an Enforce Server on Windows" on page 86.
- See "Stopping an Enforce Server on Windows" on page 86.
- See "Starting a detection server on Windows" on page 87.

- See "Stopping a detection server on Windows" on page 87.
- See "Starting services on single-tier Windows installations" on page 87.
- See "Starting services on single-tier Windows installations" on page 87.
- See "Stopping services on single-tier Windows installations" on page 88.

Starting an Enforce Server on Windows

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

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

1. On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Start the Symantec Data Loss Prevention services in the following order:
   - `SymantecDLPNotifierService`
   - `SymantecDLPManagerService`
   - `SymantecDLPIncidentPersisterService`
   - `SymantecDLPDetectionServerControllerService`

   Note: Start the `SymantecDLPNotifierService` service first before starting other services.

See "Stopping an Enforce Server on Windows" on page 86.

Stopping an Enforce Server on Windows

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

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

1. On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
   - `SymantecDLPDetectionServerControllerService`
   - `SymantecDLPIncidentPersisterService`
   - `SymantecDLPManagerService`

- SymantecDLPNotifierService

See "Starting an Enforce Server on Windows" on page 86.

Starting a detection server on Windows

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

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

See "Stopping a detection server on Windows" on page 87.

Stopping a detection server on Windows

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

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

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

See "Starting a detection server on Windows" on page 87.

Starting services on single-tier Windows installations

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

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

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Start the Symantec Data Loss Prevention in the following order:
   - SymantecDLPNotifierService
   - SymantecDLPManagerService
   - SymantecDLPIncidentPersisterService
   - SymantecDLPDetectionServerControllerService

- SymantecDLPDetectionServerService

Note: Start the SymantecDLPNotifierService service before starting other services.

See "Stopping services on single-tier Windows installations" on page 88.

Stopping services on single-tier Windows installations

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

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

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the Services menu, stop all running Symantec Data Loss Prevention services in the following order:
   - SymantecDLPDetectionServerService
   - SymantecDLPDetectionServerControllerService
   - SymantecDLPIncidentPersisterService
   - SymantecDLPManagerService
   - SymantecDLPNotifierService

See "Starting services on single-tier Windows installations" on page 87.

Chapter 6

Symantec Data Loss Prevention upgrade troubleshooting and recovery

This chapter includes the following topics:

About troubleshooting Symantec Data Loss Prevention upgrade problems

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

- See "Troubleshooting Enforce Server services" on page 90.
- See "Rolling back to the previous Symantec Data Loss Prevention release" on page 90.

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).

- Symantec Data Loss Prevention operational logs are in `C:\ProgramData\Symantec\DataLossPrevention\<EnforceServer>` or `<DetectionServer>\15.5\\logs`.
- Oracle logs can be found in `%ORACLE_BASE%\diag\rdbms\protect\protect\trace\alert_protect.log` on the Oracle server computer.

You may also need to install the Update for Universal C Runtime in Windows. See https://support.microsoft.com/en-us/kb/2999226.

Rolling back to the previous Symantec Data Loss Prevention release

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

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

- The Symantec Data Loss Prevention license file for your deployment.
- If your deployment uses Symantec Management Console, the host name or IP address of the Symantec Management Console server to use for managing Symantec Data Loss Prevention Endpoint Agents.
- A backup of the Symantec Data Loss Prevention Oracle database. For more information, see the *Symantec Data Loss Prevention System Maintenance Guide*.
- The location of the Oracle Base and Home directories.
- The Administrator credentials for your Symantec Data Loss Prevention deployment.
- The credentials for connecting to the Oracle database.
- The type of authentication that is used in your Symantec Data Loss Prevention deployment.
- The host name or IP address and port number that the Enforce Server uses to communicate with the Oracle database.

See “Reverting the Enforce Server to a previous release” on page 91.

See “Reverting a detection server to the previous release” on page 91.

Reverting the Enforce Server to a previous release

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

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

To revert an Enforce Server upgrade to the previous release

1. Stop all Symantec Data Loss Prevention services that are running on the version 15.5 Enforce Server.

   See "About Symantec Data Loss Prevention services" on page 84.

2. Disable all Symantec Data Loss Prevention services that are running on the version 15.5 Enforce Server.
3. Stop all the Oracle services.
4. Restore the Symantec Data Loss Prevention Oracle database from the latest backup.

   Consult your Oracle documentation for more information.

5. Restart all the Oracle services.

   Consult your Oracle documentation for more information.

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

   Confirm that the **Startup type** is set to **automatic** for each service.

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

Reverting a detection server to the previous release

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

See "Reverting the Enforce Server to a previous release" on page 91.

See "Rolling back to the previous Symantec Data Loss Prevention release" on page 90.

To revert a detection server upgrade to the previous release

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

   See "About Symantec Data Loss Prevention services" on page 84.

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

   Confirm that the **Startup type** is set to **automatic** for each service.

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

Creating the Enforce Reinstallation Resources file

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

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

Follow this procedure to create the `EnforceReinstallationResources.zip` file required by the Symantec Data Loss Prevention 15.5 installer.

To create the Enforce Reinstallation Resources file

1. Switch to the `\EnforceServer\15.5\Protect\bin` directory by running the following command:

   ```
   cd C:\Program
   Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\bin
   ```

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

```
"C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect\bin\
ReinstallationResourcesUtility.exe"
export C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\Protect
C:\EnforceReinstallationResources.zip
```

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

Uninstalling a server from a Windows system

To uninstall a Windows server

1. Before running the uninstaller, ensure that you have backed up all keystore files in the `C:\Program Files\Symantec\DataLossPrevention\EnforceServer\15.5\protect\keystore` directory.
2. Run the Reinstallation Resources Utility to create a backup of the `CryptoMasterKey.properties` file and the keystore files.

   See "Creating the Enforce Reinstallation Resources file" on page 92.
3. If you are uninstalling Symantec Data Loss Prevention version 15.1 and you installed version 15.5 using Silent Mode, see the Symantec Support Center article "Uninstalling Symantec Data Loss Prevention version 15.1 after upgrading to version 15.5 on Windows" for additional instructions:

   https://www.symantec.com/docs/TECH252462
4. Open the **Add or Remove Programs** control from the Windows Control Panel, select the Symantec Data Loss Prevention entry, and then click **Change/Remove**.

   The **Symantec Data Loss Prevention Uninstall** panel appears.
5. Click **Next** to uninstall Symantec Data Loss Prevention.
6. Click **Finish** to complete the uninstall process.

You can also use the following commands to uninstall Symantec Data Loss Prevention in Silent Mode:

- Run the following command to uninstall the Enforce Server:

  ```
  C:\msiexec /x EnforceServer.msi /qn /L*v c:\uninstall.log
  ```

  Run the following command to uninstall the detection server:

  ```
  C:\msiexec /x DetectionServer.msi /qn /L*v c:\uninstall.log
  ```

Chapter 7

Applying a Maintenance Pack

This chapter includes the following topics:

Applying a Symantec Data Loss Prevention Maintenance Pack

Maintenance Packs can only be applied to an already installed version of Symantec Data Loss Prevention. For example, a maintenance pack for 15.5 can only be applied to Symantec Data Loss Prevention 15.5 (new or upgraded installation).

Before applying a maintenance pack or installing Symantec Data Loss Prevention, refer to the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about system requirements. This guide is available online here:

https://www.symantec.com/docs/DOC10602

Steps to apply a maintenance pack on Windows servers

The following table describes the high-level steps that are involved in applying the maintenance pack to a Windows 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 Windows* at the Symantec Support Center at http://www.symantec.com/docs/DOC9258.

Table 7-1 Steps to apply the maintenance pack to a Windows environment

Step	Action	Description
1	Download and extract the maintenance pack software.	See "Downloading the maintenance pack software for Windows servers" on page 95.
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.	See "Updating the Enforce Server on Windows" on page 95. The process to apply the maintenance pack to a single-tier installation omits the detection server update step. See "Updating a single-tier system on Windows" on page 97.
4	Apply the maintenance pack to the detection server.	See "Updating the detection server on Windows" on page 96.

Downloading the maintenance pack software for Windows servers

Copy the MSP 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 MSP 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.msp`
- Apply the maintenance pack to the detection server: `DetectionServer.msp`
- Apply the maintenance pack to a single-tier installation: `SingleTierServer.msp`

Updating the Enforce Server on Windows

These instructions assume that Symantec Data Loss Prevention 15.5 is installed and that the `EnforceServer.msp` file has been copied into the `DLPDownloadHome` directory on the Enforce Server computer.

To update the Enforce Server

- Install the maintenance pack by completing the following steps:

  Note: You can install the maintenance pack using Silent Mode by running the following command:

  ```
  msiexec /p "EnforceServer.msp" ORACLE_PASSWORD=<ORACLE PASSWORD>/qn
  /norestart /L*v EnforceServer.log
  ```

  where <*ORACLE PASSWORD*> is the database password used for Symantec Data Loss Prevention 15.5.

  ---

  a Click **Start > Run > Browse** to navigate to the folder where you copied the `EnforceServer.msp` file.

  b Double-click `EnforceServer.msp` to execute the file, and click **OK**.

  c Click **Next** on the **Welcome** panel.

  d Enter the Symantec Data Loss Prevention database password in **Oracle Database Server Information** panel.

  e Click **Update**.

  The update process may take a few minutes. The installation program window may display for a few minutes while the services startup. After the update process completes, a completion notice displays.

Updating the detection server on Windows

These instructions assume that Symantec Data Loss Prevention 15.5 is installed and the `DetectionServer.msp` file has been copied into the `DLPDownloadHome` directory on the detection server computer.

To update the detection server

- Install the maintenance pack by completing the following steps:

  Note: You can install the maintenance pack using Silent Mode by running the following command:

  ```
  msiexec /p "DetectionServer.msp" /qn /norestart /L*v DetectionServer.log
  ```

  a. Click **Start > Run > Browse** to navigate to the folder where you copied the `DetectionServer.msp` file.

  b. Double-click `DetectionServer.msp` to execute the file, and click **OK**.

  c. Click **Next** on the **Welcome** panel.

  d. Click **Update**.

  The update process may take a few minutes. The installation program window may display for a few minutes while the services startup. After the update process completes, a completion notice displays.

Updating a single-tier system on Windows

The following instructions assume that the `SingleTierServer.msp` file has been copied into the `DLPDownloadHome` directory on the Enforce Server computer.

To update a single-tier system

- Install the maintenance pack by completing the following steps:

Note: You can install the maintenance pack using Silent Mode by running the following command:

```
msiexec /p "SingleTierServer.msp" ORACLE_PASSWORD=<ORACLE PASSWORD>/qn
/norestart /L*v EnforceServer.log
```

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

---

a Click **Start > Run > Browse** to navigate to the folder where you copied the `SingleTierServer.msp` file.

b Double-click `SingleTierServer.msp` to execute the file, and click **OK**.

c Click **Next** on the **Welcome** panel.

d Enter the Symantec Data Loss Prevention database password in **Oracle Database Server Information** panel.

e Click **Update**.

The update process may take a few minutes. The installation program window may display for a few minutes while the services startup. After the update process completes, a completion notice displays.

Index

U

V