Symantec™ Data Loss Prevention Installation Guide for Windows

Version 15.0

Symantec Data Loss Prevention Installation Guide for Windows

Documentation version: 15.0a

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Planning the Symantec Data Loss Prevention installation

This chapter includes the following topics:

About installation tiers

Symantec Data Loss Prevention supports three different installation types: three-tier, two-tier, and single-tier. Symantec recommends the three-tier installation. However, your organization might need to implement a two-tier installation depending on available resources and organization size. Single-tier installations are recommended for branch offices, small organizations, or for testing purposes.

Single-tier

To implement the single-tier installation, you install the database, the Enforce Server, and a detection server all on the same computer. Typically, this installation is implemented for testing purposes.

A Symantec Data Loss Prevention Single Server deployment is a single-tier deployment that includes the **Single Tier Monitor** detection server. The **Single Tier Monitor** is a detection server that includes the detection capabilities of the Network Monitor, Network Discover, Network Prevent for Email, Network Prevent for Web, and the Endpoint Prevent and Endpoint Discover detection servers. Each of these detection server types is associated with one or more detection "channels." The Single Server deployment simplifies Symantec Data Loss Prevention administration and reduces maintenance and hardware costs for small organizations, or for branch offices of larger enterprises that would benefit from on-site deployments of Symantec Data Loss Prevention.

If you choose either of these types of installation, the Symantec Data Loss Prevention administrator needs to be able to perform database maintenance tasks, such as database backups.

See “Performing a single-tier installation—high-level steps” on page 17.

See “Installing an Enforce Server” on page 23.

See “Registering a detection server” on page 45.

Two-tier

To implement the two-tier installation, you install the Oracle database and the Enforce Server on the same computer. You then install detection servers on separate computers.

Typically, this installation is implemented when an organization, or the group responsible for data loss prevention, does not have a separate database administration team. If you choose this type of installation, the Symantec Data Loss Prevention administrator needs to be able to perform database maintenance tasks, such as database backups.

See “Performing a two-tier installation—high-level steps” on page 15.

Three-tier	To implement the three-tier installation, you install the Oracle database, the Enforce Server, and a detection server on separate computers. Symantec recommends implementing the three-tier installation architecture as it enables your database administration team to control the database. In this way you can use all of your corporate standard tools for database backup, recovery, monitoring, performance, and maintenance. Three-tier installations require that you install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server to communicate with the Oracle server. See "Performing a three-tier installation—high-level steps" on page 13.

About single sign-on

Symantec Data Loss Prevention provides several options for authenticating users and signing users on to the Enforce Server administration console. The Symantec Data Loss Prevention installation program helps you configure several of these options when you install the Enforce Server. These installation options include:

- Password authentication with forms-based sign-on.
  This is the default method of authenticating users to the Enforce Server administration console. When using password authentication, users sign on to the Enforce Server administration console by accessing the sign-on page in their browser and entering their user name and password. You can enable password authentication in addition to certificate authentication.
- Certificate authentication.
  Symantec Data Loss Prevention supports single sign-on using client certificate authentication. With certificate authentication, a user interacts with a separate public key infrastructure (PKI) to generate a client certificate that Symantec Data Loss Prevention supports for authentication. When a user accesses the Enforce Server administration console, the PKI automatically delivers the user's certificate to the Enforce Server computer for authentication and sign-on. If you choose certificate authentication, the installation program gives you the option to enable password authentication as well.

If you want to enable certificate authentication, first verify that your client certificates are compatible with Symantec Data Loss Prevention. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*. Certificate authentication also requires that you install the certificate authority (CA) certificates that are necessary to validate client certificates in your system. These certificates must be available in `.cer` files on the Enforce Server computer. During the Symantec Data Loss Prevention installation, you can import these CA certificates if available.

If you want to use password authentication, no additional information is required during the Symantec Data Loss Prevention installation.

See “About authenticating users” in the *Symantec Data Loss Prevention Administration Guide* for more information about all of the authentication and sign-on mechanisms that Symantec Data Loss Prevention supports.

See the *Symantec Data Loss Prevention Administration Guide* for information about configuring certificate authentication after you install Symantec Data Loss Prevention.

About hosted Network Prevent deployments

Symantec Data Loss Prevention supports deploying one or more Network Prevent detection servers in a hosted service provider network, or in a network location that requires communication across a Wide Area Network (WAN). You may want to deploy a Network Prevent server in a hosted environment if you use a service provider's mail server or Web proxy. In this way, the Network Prevent server can be easily integrated with the remote proxy to prevent confidential data loss through email or HTTP posts.

You can deploy the Enforce Server and detection servers to the Amazon Web Services infrastructure. For details, see https://support.symantec.com/en_US/article.DOC9520.html.

When you choose to install a detection server, the Symantec Data Loss Prevention installation program asks if you want to install Network Prevent in a hosted environment.

See “Installing a detection server” on page 40.

If you choose to install a Network Prevent detection server in a hosted environment, you must use the `sslkeytool` utility to create multiple, user-generated certificates to use with both internal (corporate) and hosted detection servers. This ensures secure communication from the Enforce Server to the hosted Network Prevent server, and to all other detection servers that you install. You cannot use the built-in Symantec Data Loss Prevention certificate when you deploy a hosted Network Prevent detection server.

See “Using sslkeytool to generate new Enforce and detection server certificates” on page 52.

The *Symantec Data Loss Prevention Installation Guide* describes how to install and configure the Network Prevent server in either a LAN environment or a hosted environment.

About Symantec Data Loss Prevention system requirements

System requirements for Symantec Data Loss Prevention depend on:

- The type of information you want to protect
- The size of your organization
- The number of Symantec Data Loss Prevention servers you choose to install

- The location in which you install the servers

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for detailed information.

Symantec Data Loss Prevention required items

Refer to the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for detailed requirements information. Before you install Symantec Data Loss Prevention, make sure that the following items are available:

- Your Symantec Data Loss Prevention software.
  Download and extract the Symantec Data Loss Prevention software ZIP files. Extract these ZIP files 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. Refer to the *Acquiring Symantec Data Loss Prevention Software* document for more information.
- Your Symantec Data Loss Prevention license file.
  Download your Symantec Data Loss Prevention license file into a directory on a system that is accessible to you. License files have names in the format `name.slf`. Refer to the *Acquiring Symantec Data Loss Prevention Software* document for more information.
- The Oracle database software. You can find this software in the Symantec Data Loss Prevention installation package.
  Install Oracle software before installing the Enforce Server. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* or the *Symantec Data Loss Prevention Oracle 12c Implementation Guide* for details.
- The following third-party components, if required:
  - Network Monitor servers require either a dedicated NIC or a high-speed packet capture adapter. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for requirements.
  - Windows-based Network Monitor servers require WinPcap software. WinPcap software is recommended for all detection servers. Locate the WinPcap software at the following URL:
    http://www.winpcap.org/
    See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for version requirements.
  - Wireshark, available from Wireshark. During the Wireshark installation process on Windows platforms, do not install a version of WinPcap lower than 4.1.2.
  - For two-tier or three-tier installations, a remote access utility may be required (for example, Remote Desktop for Windows systems, or PuTTY or a similar SSH client for Linux systems).

- Windows-based Discover servers that are scanning targets on UNIX machines require Windows Services for UNIX (SFU) 3.5.
  SFU enables you to access UNIX services from Windows. You can download this software from Windows Services for UNIX Version 3.5 at the Microsoft Download Center.
  Install SFU on Discover servers that will scan UNIX machines.
- Adobe Reader (for reading Symantec Data Loss Prevention documentation).

Standard ASCII characters required for all installation parameters

Use only standard, 7-bit ASCII characters to enter installation parameters during the installation process. Extended (hi-ASCII) and double-byte characters cannot be used for account or user names, passwords, directory names, IP addresses, or port numbers. Installation may fail if you use characters other than standard 7-bit ASCII.

Note also that installation directories cannot contain any spaces in the full path name. For example, `c:\Program Files\SymantecDLP` is not a valid installation folder because there is a space between "Program" and "Files."

Performing a three-tier installation—high-level steps

The computer on which you install Symantec Data Loss Prevention must contain only the software that is required to run the product. Symantec does not support installing Symantec Data Loss Prevention on a computer with unrelated applications.

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for a list of required and recommended third-party software.

Table 1-1 Performing a three-tier installation—high-level steps

Step	Action	Description
1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 19.
2	Verify that your servers are ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.

Table 1-1 Performing a three-tier installation—high-level steps *(continued)*

Step	Action	Description
3	Install Oracle and create the Symantec Data Loss Prevention database.	In a three-tier installation your organization's database administration team installs, creates, and maintains the Symantec Data Loss Prevention database. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* or the *Symantec Data Loss Prevention Oracle 12c Implementation Guide* for information about installing Oracle.
4	Install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server computer to enable communication with the Oracle server.	The user account that is used to install Symantec Data Loss Prevention requires access to SQL*Plus to create tables and views. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for information about installing the Oracle client software.
5	Install the Enforce Server.	See "Installing an Enforce Server" on page 23.
6	Verify that the Enforce Server is correctly installed.	See "Verifying an Enforce Server installation" on page 31.
7	Import a solution pack.	See "Importing a solution pack" on page 33. See "About Symantec Data Loss Prevention solution packs" on page 32.

Table 1-1 Performing a three-tier installation—high-level steps *(continued)*

Step	Action	Description
8	Generate server certificates for secure communication.	If you are installing Network Prevent in a hosted environment, you must create user-generated certificates for the Enforce Server and all detection servers in your deployment. This ensures that communication between the Enforce Server and all detection servers is secure. Symantec recommends that you generate new certificates for any multi-tier deployment. If you do not generate new certificates, Enforce and detection servers use a default, built-in certificate that is shared by all Symantec Data Loss Prevention installations. See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.
9	Install a detection server.	See "Installing a detection server" on page 40.
10	Register a detection server.	See "Registering a detection server" on page 45.
12	Perform the post-installation tasks.	See "About post-installation tasks" on page 111.
13	Start using Symantec Data Loss Prevention to perform initial setup tasks; for example, change the Administrator password, and create user accounts and roles.	See "About post-installation security configuration" on page 112. For more detailed administration topics (including how to configure a specific detection server) see the *Symantec Data Loss Prevention Administration Guide*.

Performing a two-tier installation—high-level steps

The computer on which you install Symantec Data Loss Prevention must only contain the software that is required to run the product. Symantec does not support installing Symantec Data Loss Prevention on a computer with unrelated applications.

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for a list of required and recommended third-party software.

Table 1-2 Performing a two-tier installation—high-level steps

Step	Action	Description
1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 19.
2	Verify that your servers are ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.
3	Install Oracle and create the Symantec Data Loss Prevention database.	See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* or the *Symantec Data Loss Prevention Oracle 12c Implementation Guide*.
4	Install the Enforce Server.	See "Installing an Enforce Server" on page 23.
5	Verify that the Enforce Server is correctly installed.	See "Verifying an Enforce Server installation" on page 31.
6	Import a solution pack.	See "About Symantec Data Loss Prevention solution packs" on page 32. See "Importing a solution pack" on page 33.

Table 1-2 Performing a two-tier installation—high-level steps *(continued)*

Step	Action	Description
7	Generate server certificates for secure communication.	If you are installing Network Prevent in a hosted environment, you must create user-generated certificates for the Enforce Server and all detection servers in your deployment. This ensures that communication between the Enforce Server and all detection servers is secure. Symantec recommends that you generate new certificates for any multi-tier deployment. If you do not generate new certificates, Enforce and detection servers use a default, built-in certificate that is shared by all Symantec Data Loss Prevention installations. See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.
8	Install a detection server.	See "Installing a detection server" on page 40.
9	Register a detection server.	See "Registering a detection server" on page 45.
11	Perform the post-installation tasks.	See "About post-installation tasks" on page 111.
12	Start using Symantec Data Loss Prevention to perform initial setup tasks; for example, change the Administrator password, and create user accounts and roles.	See "About post-installation security configuration" on page 112. For more detailed administration topics (including how to configure a specific detection server) see the *Symantec Data Loss Prevention Administration Guide*.

Performing a single-tier installation—high-level steps

Single-tier installations are for testing, training, and risk assessment purposes.

A single-tier installation that is used in production is called a Single Server deployment. Single Server deployments are for branch offices or small organizations.

The computer on which you install Symantec Data Loss Prevention must only contain the software that is required to run the product. Symantec does not support installing Symantec Data Loss Prevention on a computer with unrelated applications.

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for a list of required and recommended third-party software.

Table 1-3 Performing a single-tier installation—high-level steps

Step	Action	Reference
1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 19.
2	Verify that the server is ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.
3	Install Oracle and create the Symantec Data Loss Prevention database.	See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* or the *Symantec Data Loss Prevention Oracle 12c Implementation Guide*.
4	Install the Enforce Server and a detection server on the same computer.	See "Installing a single-tier server " on page 65.
5	Verify that the Enforce Server is correctly installed.	See "Verifying a single-tier installation" on page 74.
6	Import a solution pack.	See "About Symantec Data Loss Prevention solution packs" on page 32. See "Importing a solution pack" on page 33.
7	Register the detection server.	See "Registering a detection server" on page 45.
8	Perform the post-installation tasks.	See "About post-installation tasks" on page 111.
9	Start using Symantec Data Loss Prevention to perform initial setup tasks; for example, change the Administrator password, and create user accounts and roles.	See "About post-installation security configuration" on page 112. For more detailed administration topics (including how to configure a specific detection server) see the *Symantec Data Loss Prevention Administration Guide*.

Symantec Data Loss Prevention preinstallation steps

This section assumes that the following tasks have been completed:

- You have verified that the server meets the system requirements.
  See "About Symantec Data Loss Prevention system requirements" on page 11.
- You have gathered the required materials.
  See "Symantec Data Loss Prevention required items" on page 12.

To prepare to install a Symantec Data Loss Prevention server

1. Review the Release Notes for installation, Windows versus Linux capabilities, and server-specific information before beginning the installation process.
2. Make sure your server is up to date with the latest Windows security patches.
3. Obtain the Administrator user name and password for each system on which Symantec Data Loss Prevention is to be installed.
4. Obtain the static IP address(es) for each system on which Symantec Data Loss Prevention is to be installed.
5. Verify that each server host name that you will specify has a valid DNS entry.
6. Verify that you have access to all remote computers that you will use during the installation (for example, by using Terminal Services, Remote Desktop, or an SSH client).
7. Verify the Microsoft Windows server installation.

   See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.
8. If you want to store your incident attachments on an external file system rather than in the Oracle database, ensure that you have set up your external storage directory and know the path to that location.

   See "About external storage for incident attachments" on page 20.
9. Copy the following files from *DLPDownloadHome* to an easily accessible directory on the Enforce Server:
   - Symantec Data Loss Prevention installer: `ProtectInstaller64_15.0.exe`.
     This file can be found in the *DLPDownloadHome*`\DLP\15.0\New_Installs\x64` directory.
   - Your Symantec Data Loss Prevention license file.
     License files have names in the format *name*`.slf`.
   - Symantec DLP Agent installers
     These files can be found in the following locations:
     - Mac installer:
       DLPDownloadHome`\DLP\15.0\Endpoint\Mac\x86_64\AgentInstall_15_0.pkg`

- Windows 64-bit:
  DLPDownloadHome\DLP\15.0\Endpoint\Win\x64\AgentInstall64_15_0.msi
- Windows 32-bit:
  DLPDownloadHome\DLP\15.0\Endpoint\Win\x86\AgentInstall_15_0.msi.

These files are only available if you licensed Endpoint Prevent.

10 If you plan to use Symantec Data Loss Prevention alerting capabilities, you need the following items:

- Access to a local SMTP server.
- Mail server configuration for sending SMTP email. This configuration includes an account and password if the mail server requires authentication.

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 an stand-alone computer. You can use any file system you choose. Symantec recommends that you work with your data storage administrator to set up an appropriate directory for incident attachment storage.

To set up an external storage directory, Symantec recommend these best practices:

- If you choose to store your incident attachments on the Enforce Server host computer, do not place your storage directory under the /SymantecDLP folder.
- If you choose to store incident attachments on a computer other than your Enforce Server host computer, take the following steps:
  - Ensure that both the external storage server and the Enforce Server are in the same domain.
  - Create a "protect" user with the same password as your Enforce Server "protect" user to use with your external storage directory.
  - If you are using a Linux system for external storage, change the owner of the external storage directory to the external storage "protect" user.
  - If you are using a Microsoft Windows system for external storage, share the directory with Read/Writer permissions with the external storage "protect" user.

After you have set up your storage location you can enable external storage for incident attachments in the Installation Wizard. All incident attachments will be stored in the external

storage directory. Incident attachments in the external storage directory cannot be migrated back to the database. All incidents 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.

Verifying that servers are ready for Symantec Data Loss Prevention installation

Before installing Symantec Data Loss Prevention, you must verify that the server computers are ready.

To verify that servers are ready for Symantec Data Loss Prevention installation

1. Verify that all systems are racked and set up in the data center.
2. Verify that the network cables are plugged into the appropriate ports as follows:
   - Enforce Server NIC Port 1.
     Standard network access for Administration.
     If the Enforce Server has multiple NICs, disable the unused NIC if possible. This task can only be completed once you have installed the Enforce Server.
     See "Enforce Servers and unused NICs" on page 127.
   - Detection servers NIC Port 1.
     Standard network access for Administration.
   - Network Monitor detection servers NIC Port 2.
     SPAN port or tap should be plugged into this port for detection. (Does not need an IP address.)
     If you use a high-speed packet capture card (such as Endace or Napatech), then do not set this port for SPAN or tap.
3. Log on as the Administrator user.
4. Assign a static IP address, subnet mask, and gateway for the Administration NIC on the Enforce Server. Do not assign an IP address to the detection server NICs.
5. Make sure that the management NIC has the following items enabled:
   - Internet protocol TCP/IP
   - File and Printer Sharing for Microsoft networks
   - Client for Microsoft Networks

Disabling any of these can cause communication problems between the Enforce Server and the detection servers.

6 From a command line, use `ipconfig /all` to verify assigned IP addresses.

7 If you do not use DNS, check that the `c:\windows\system32\drivers\etc\hosts` file contains the server name and IP addresses for the server computer. If you modify this file, restart the server to apply the changes.

8 If you are using DNS, verify that all host names have valid DNS entries.

9 Ping each Symantec Data Loss Prevention server computer (using both IP and host name) to verify network access.

10 Verify that ports 443 (SSL) and 3389 (RDP) are open and accessible to the client computers that require access.

11 Turn on remote desktop connections for each Symantec Data Loss Prevention server computer. In Windows, right-click **My Computer**. Click **Properties** and then select **Remote > Allow users to connect remotely to this computer**. Verify that you can use Remote Desktop to log onto the server from a local workstation.

12 Verify that port 25 is not blocked. The Symantec Data Loss Prevention server uses port 25 (SMTP) for email alerts.

13 Verify that the Network Monitor detection server NICs receive the correct traffic from the SPAN port or tap. Install the latest version of Wireshark and use it to verify traffic on the server.

For Endace cards, use `dagsnap -o out.pcap` from a command line. Then review the dagsnap output in Wireshark.

For Napatech cards, there is a "statistics" tool with option `-bch=0xf` to observe the "Hardware counters" for all channels/ports.

14 Ensure that all servers are synchronized with the same time (to the minute). Ensure that the servers are updated with the correct Daylight Saving Time patches.

See "Symantec Data Loss Prevention required items" on page 12.

See "Symantec Data Loss Prevention preinstallation steps" on page 19.

For Network Prevent for Email detection server installations, verify the following:

- Use an SSH client to verify that you can access the Mail Transfer Agent (MTA).
- Verify that the firewall permits you to Telnet from the Network Prevent for Email Server computer to the MTA on port 25. Also ensure that you can Telnet from the MTA to the Network Prevent for Email detection server computer on port 10026.

Chapter 2

Installing an Enforce Server

This chapter includes the following topics:

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server.

Before you install an Enforce Server:

- Complete the preinstallation steps.
  See "Symantec Data Loss Prevention preinstallation steps" on page 19.
- Verify that the system is ready for installation.
  See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.
- Ensure that the Oracle software and Symantec Data Loss Prevention database is installed on the appropriate system.
  - For single- and two-tier Symantec Data Loss Prevention installations, Oracle is installed on the same computer as the Enforce Server.
  - For a three-tier installation, Oracle is installed on a separate server. For a three-tier installation, the Oracle Client (SQL*Plus and Database Utilities) must be installed on the Enforce Server computer to enable communication with the Oracle server.

  See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for details.
- Before you begin, make sure that you have access and permission to run the Symantec Data Loss Prevention installer software: `ProtectInstaller64_15.0.exe`.

If you intend to run Symantec Data Loss Prevention using Federal Information Processing Standards (FIPS) encryption, you must first prepare for FIPS encryption. You must also run the ProtectInstaller with the appropriate FIPS parameter.

See "About FIPS encryption" on page 139.

Note: The following instructions assume that the `ProtectInstaller64_15.0.exe` file and license file have been copied into the `c:\temp` directory on the Enforce Server computer.

To install an Enforce Server

1. Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.
2. Log on (or remote log on) as Administrator to the Enforce Server system on which you intend to install Enforce.
3. Go to the folder where you copied the `ProtectInstaller64_15.0.exe` file (`c:\temp`).
4. Double-click `ProtectInstaller64_15.0.exe` to execute the file, and click **OK**.
5. In the **Welcome** panel, click **Next**.
6. After you review the license agreement, select **I accept the agreement**, and click **Next**.
7. In the **Select Components** panel, select the type of installation you are performing and then click **Next**.

   There are four choices:

   - **Enforce**
     Select **Enforce** to install Symantec Data Loss Prevention on an Enforce Server for two- or three-tier installations. When you select **Enforce**, the Indexer is also automatically selected by default.
   - **Detection**
     Select **Detection** to install a detection server as part of a two- or three-tier installation.
   - **Indexer**
     Select **Indexer** to install a remote indexer.
   - **Single Tier**
     Select **Single Tier** to install all components on a single system.
     Single-tier systems are for branch offices or small organizations, or for testing, training, and risk assessment.

   Because these are the instructions for installing an Enforce Server, choose **Enforce**.

8 In the **License File** panel, browse to the directory containing your license file. Select the license file, and click **Next**.

License files have names in the format *name*.slf.

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

```
c:\SymantecDLP
```

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.

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.

Note: Do not install Symantec Data Loss Prevention in any directory that includes spaces in its path. For example, `c:\Program Files\SymantecDLP` is not a valid installation folder because there is a space between “Program” and “Files.”

---

10 In the **Select Start Menu Folder** panel, enter the Start Menu folder where you want the Symantec Data Loss Prevention shortcuts to appear.

The default is `Symantec Data Loss Prevention`.

11 Select one of the following options and then click **Next**.

- **Create shortcuts for all users**
  The shortcuts are available in the same location for all users of the Enforce Server.
- **Don’t create a Start Menu folder**
  The Symantec Data Loss Prevention shortcuts are not available from the Start menu.

12 In the **System Account** panel, select one of the following options: Then click **Next**.

- **Create a new service user**: 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 “protect.” New service user accounts are 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.

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

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 **Transport Configuration** panel (this panel only appears when during single-tier installations), enter an unused port number that Symantec Data Loss Prevention servers can use to communicate with each other and click **Next**. The default port is 8100.

16 In the **Oracle Database Server Information** panel, enter the location of the Oracle database server. Specify one of the following options in the **Oracle Database Server** field:

- 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.

17 Enter the **Oracle Listener Port**, or accept the default, and click **Next**.

18 In the **Oracle Database User Configuration** panel, enter the Symantec Data Loss Prevention database user name and password. Enter the database SID (typically “protect”), then click **Next**.

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.

See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.

If you are re-using a database that was created for an earlier Symantec Data Loss Prevention installation, the Symantec Data Loss Prevention database user ("protect" user by default) may not have sufficient privileges to install the product. In this case, you must manually add the necessary privileges using SQL*Plus. See the *Symantec Data Loss Prevention Upgrade Guide* for your platform.

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.

---

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 Select one of the following options in the **Initialize DLP Database** panel:

- For a new Symantec Data Loss Prevention installation, make sure that the **Initialize Enforce Data** box is checked and then click **Next**.
  You can also check this box if you are reinstalling and want to overwrite the existing Enforce schema and all data. Note that this action cannot be undone. If this check box is selected, the data in your existing Symantec Data Loss Prevention database is destroyed after you click **Next**.
- Clear the **Initialize Enforce Data** check box if you want to perform a recovery operation. Clearing the check box skips the database initialization process. If you choose skip the database initialization, you must specify the unique `CryptoMasterKey.properties` file for the existing database that you want to use.

21 If you selected either **Symantec Protection Console** or **None** as your log on option, skip this step.

In the **Import Certificates** panel, select options for certificate authentication, then click **Next**:

Option	Description
Import Certificates **Select Certificate Directory**	Select **Import Certificates** if you want to import certificate authority (CA) certificates during the Enforce Server installation. CA certificates are required to validate client certificates when you choose **Certificate Authentication** sign on. If the necessary CA certificates are available on the Enforce Server computer, select **Import Certificates** and click **Browse** to navigate to the directory where the `.cer` files are located. Uncheck **Import Certificates** if the necessary certificates are not available on the Enforce Server computer, or if you do not want to import certificates at this time. You can import the required certificates after installation using instructions in the *Symantec Data Loss Prevention Administration Guide*.
Allow Form Based Authentication	Select this option if you want to support password authentication with forms-based sign-on in addition to single sign-on with certificate authentication. Symantec recommends that you select option this as a backup option while you configure and test certificate authentication with your PKI. You can disable password authentication and forms-based sign-on after you have validated that certificate authentication is correctly configured for your system.

22 If you chose to initialize the Enforce Server database, skip this step.

If you chose to re-use an existing Enforce Server database, the installer displays the **Load Reinstallation Resources** panel. Click **Browse** and navigate to select the `EnforceReinstallationResources.zip` file from your previous installation.

Click **Next** to continue the installation.

23 If you chose to re-use an existing Enforce Server database, skip this step.

In the **Administrator Credentials** panel, specify information according to the sign-on option that you selected:

Option	Description
Password **Re-enter Password**	If you chose an option to support password authentication with forms-based log on, enter a password for the Enforce Server Administrator account in both the **Password** and **Re-enter Password** fields. The Administrator password must contain a minimum of eight characters. You can change the Administrator password from the Enforce Server administration console at any time. **Note:** These fields are not displayed if you selected **Certificate Authentication** but you did not select **Allow Form Based Authentication**. In this case, you must log on to the Enforce Server administration console using a client certificate that contains the administrator's common name value.
Common Name (CN)	If you chose to support certificate authentication, enter the Common Name (CN) value that corresponds to the Enforce Server Administrator user. The Enforce Server will assign administrator privileges to the user who logs on with a client certificate that contains this CN value. **Note:** This field is displayed only if you selected **Certificate Authentication**.

24 Click **Next**.

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

25 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.

26 Click **Next**.

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

27 Confirm your participation in the Symantec Data Loss Prevention Supportability Telemetry program, and provide the appropriate information.

The Symantec Data Loss Prevention Supportability Telemetry Program can significantly improve the quality of Symantec Data Loss Prevention. For more information, click the Supportability and Telemetry Program Details link.

28 Click **Next**.

The installation process begins. After the Installation Wizard extracts the files, it connects to the database using the name and password that you entered earlier. The wizard then creates the database tables. If any problems with the database are discovered, a notification message displays.

The **Installing** panel appears, and displays a progress bar.

29 Select the **Start Services** check box to start the Symantec Data Loss Prevention services after the after the completion notice displays.

The services can also be started or stopped using the Windows Services utility.

30 Click **Finish**.

Starting all of the services can take up to a minute. The installation program window may persist for a while, during the startup of the services. After a successful installation, a completion notice displays.

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

32 Verify that the Enforce Server is properly installed.

See "Verifying an Enforce Server installation" on page 31.

33 Import a Symantec Data Loss Prevention solution pack immediately after installing the Enforce Server, and before installing any detection servers.

See "About Symantec Data Loss Prevention solution packs" on page 32.

34 Back up the unique `CryptoMasterKey.properties` file for your installation and store the file in a safe place. This file is required for Symantec Data Loss Prevention to encrypt and decrypt the Enforce Server database.

Note: 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.

Verifying an Enforce Server installation

After installing an Enforce Server, verify that it is operating correctly before importing a solution pack.

To verify the Enforce Server installation

1. Confirm that Oracle Services (OracleOraDb11g_home1TNSListener and OracleServicePROTECT) automatically start upon system restart.
2. If you selected the option **Start Services**, then confirm that all of the Symantec Data Loss Prevention Services are running under the System Account user name that you specified during installation.

   Note that on Windows platforms, all services run under the System Account user name (by default, “protect”), except for the `VontuUpdate` services, which run *username*_update (by default, “protect_update”).

   Symantec Data Loss Prevention includes the following services:

   - `VontuManager`
   - `VontuIncidentPersister`
   - `VontuNotifier`
   - `VontuUpdate`
   - `VontuMonitorController`
3. If the Symantec Data Loss Prevention services do not start, check the log files for possible issues (for example, connectivity, password, or database access issues).

   - The Symantec Data Loss Prevention installation log is `c:\SymantecDLP\.install4j\installation.log`.
   - Symantec Data Loss Prevention operational logs are in `c:\SymantecDLP\Protect\logs`.
   - Oracle logs can be found in `c:\app\Administrator\admin\protect` 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.
4. Once you have verified the Enforce Server installation, you can log on to the Enforce Server to view the administration console. Using the administration console, go to **System > Settings > General** accept the EULA, enter your company information, and confirm that all of your licenses have been correctly activated.

   See the *Symantec Data Loss Prevention Administration Guide* for information about logging on to, and using, the Enforce Server administration console.

Chapter 3

Importing a solution pack

This chapter includes the following topics:

About Symantec Data Loss Prevention solution packs

You import a solution pack to provide the initial Enforce Server configuration. Each solution pack includes policies, roles, reports, protocols, and the incident statuses that support a particular industry or organization.

Solution packs have file names ending in `*.vsp` (for example, `Energy_v15.0.vsp`).

Download the `Symantec_DLP_15.0_Solution_Packs.zip` from https://fileconnect.symantec.com to the same local system you downloaded other Data Loss Prevention components.

Unzip the solution pack `Symantec_DLP_15.0_Solution_Packs.zip` file contents to the *`DLPDownloadHome`*`\DLP\15.0\Solution_Packs\` directory.

Symantec provides the solution packs listed in Table 3-1.

Table 3-1 Symantec Data Loss Prevention solution packs

Name	File name
Energy & Utilities Solution Pack	Energy_v15.0.vsp
EU and UK Solution Pack	EU_UK_v15.0.vsp
Federal Solution Pack	Federal_v15.0.vsp
Financial Services	Financial_v15.0.vsp
Health Care Solution Pack	Health_Care_v15.0.vsp

Table 3-1 Symantec Data Loss Prevention solution packs *(continued)*

Name	File name
High Tech Solution Pack	High_Tech_v15.0.vsp
Insurance Solution Pack	Insurance_v15.0.vsp
Manufacturing Solution Pack	Manufacturing_v15.0.vsp
Media & Entertainment Solution Pack	Media_Entertainment_v15.0.vsp
Pharmaceutical Solution Pack	Pharmaceutical_v15.0.vsp
Retail Solution Pack	Retail_v15.0.vsp
Telecom Solution Pack	Telecom_v15.0.vsp
General Solution Pack	Vontu_Classic_v15.0.vsp

See the solution pack documentation for a description of the contents of each solution pack.

Solution pack documentation can be found in the following directory:

DLPDownloadHome\DLP\15.0\Docs\Solution_Packs\.

This directory was created when you unzipped either the entire software download file or the documentation ZIP file.

You must choose and import a solution pack immediately after installing the Enforce Server and before installing any detection servers. You only import a single solution pack. You cannot change the imported solution pack at a later time.

See "Importing a solution pack" on page 33.

For information about importing a solution pack, see the *Symantec Data Loss Prevention Installation Guide*.

Importing a solution pack

You import a Symantec Data Loss Prevention solution pack on the Enforce Server computer. The following rules apply when you import a solution pack:

- You must import the solution pack immediately after you install the Enforce Server and before you install any detection server. (If you performed a single-tier installation, you must import the solution pack immediately after the installation is complete.)
- Only import a solution pack that was created for the specific Enforce Server version you installed. Do not import a solution pack that was released with a previous version of the Symantec Data Loss Prevention software.

For example, do not import a version 14.6 solution pack on a version 15.0 Enforce Server.

- Do not attempt to import more than one solution pack on the same Enforce Server, as the solution pack import fails.
- Do not import a solution pack on an Enforce Server that was modified after the initial installation; the solution pack import fails.
- After you import a solution pack, you cannot change the installation to use a different solution pack at a later time.

To import a solution pack

1. Decide which solution pack you want to use.

   See "About Symantec Data Loss Prevention solution packs" on page 32.

   Note: You must use a version 15.0 solution pack; earlier versions are not supported.

2. Log on (or remote log on) as Administrator to the Enforce Server computer.
3. Copy the solution pack file from *DLPDownloadHome*\DLP\15.0\Solution_Packs\ to an easily accessible local directory.
4. In Windows Services, stop the SymantecDLPManager service.

   See "About Symantec Data Loss Prevention services" on page 129.

5. From the command-line prompt, change to the \SymantecDLP\protect\bin directory on the Enforce Server. This directory contains the SolutionPackInstaller.exe application. For example:

   ```
   cd c:\SymantecDLP\Protect\bin
   ```

6. Import the solution pack by running SolutionPackInstaller.exe from the command line and specifying the solution pack directory path and file name. The solution pack directory must not contain spaces.

   For example, if you placed a copy of the Financial_v15.0.vsp solution pack in the \SymantecDLP directory of the Enforce Server, you would enter:

```
SolutionPackInstaller.exe import c:\SymantecDLP\Financial_v15.0.vsp
```

7. Check the solution pack installer messages to be sure that the installation succeeded without error.

8 Restart the `SymantecDLPManager` service.

See “About Symantec Data Loss Prevention services” on page 129.

9 After you have completed importing the solution pack, do one of the following depending on the type of installation:

- On three-tier or two-tier installations install one or more detection servers.
  See “About detection servers” on page 36.
  See “Installing a detection server” on page 40.
- On a single-tier installation register a detection server.
  See “Registering a detection server” on page 45.
  See “Verifying a detection server installation” on page 44.

Chapter 4

Installing and registering detection servers

This chapter includes the following topics:

About detection servers

The Symantec Data Loss Prevention suite includes the types of detection servers described in Table 4-1. The Enforce Server manages all of these detection servers.

For information about registering cloud detectors, see the *Symantec Data Loss Prevention Administration Guide* or the documentation that accompanies your cloud detector.

Table 4-1 Detection servers

Server Name	Description
Network Monitor	Network Monitor inspects the network communications for confidential data, accurately detects policy violations, and precisely qualifies and quantifies the risk of data loss. Data loss can include intellectual property or customer data.

Table 4-1 Detection servers *(continued)*

Server Name	Description
Network Discover/Cloud Storage Discover	Network Discover/Cloud Storage Discover identifies unsecured confidential data that is exposed on open file shares, web servers, Microsoft Exchange servers, Microsoft SharePoint, and Box cloud collaboration platforms. Network Protect reduces your risk by removing exposed confidential data, intellectual property, and classified information from open file shares on network servers or desktop computers. Note that there is no separate Network Protect server; the Network Protect product module adds protection functionality to the Network Discover/Cloud Storage Discover Server.
Network Prevent for Email	Network Prevent for Email prevents data security violations by blocking the email communications that contain confidential data. It can also conditionally route traffic with confidential data to an encryption gateway for secure delivery and encryption-policy enforcement. **Note:** You can optionally deploy Network Prevent for Email in a hosted service provider network, or in a network location that requires communication across a Wide Area Network (WAN) to reach the Enforce Server. See "About hosted Network Prevent deployments" on page 11.
Network Prevent for Web	Network Prevent for Web prevents data security violations for data that is transmitted by web communications and file-transfer protocols. **Note:** You can optionally deploy Network Prevent for Web in a hosted service provider network, or in a network location that requires communication across a Wide Area Network (WAN) to reach the Enforce Server. See "About hosted Network Prevent deployments" on page 11.
Endpoint Prevent	Endpoint Prevent monitors the use of sensitive data on endpoint systems and detects endpoint policy violations. Endpoint Prevent also identifies unsecured confidential data that is exposed on endpoints.
Single Tier Monitor	The Single Tier Monitor enables the detection servers that you have licensed on the same host as the Enforce Server. The single-tier server performs detection for the following products (you must have a license for each): Network Monitor, Network Discover/Cloud Storage Discover, Network Prevent for Email, Network Prevent for Web, and Endpoint Prevent.

See "Detection servers and remote indexers" on page 38.

See "Detection server installation preparations" on page 38.

See “Installing a detection server” on page 40.

See “Verifying a detection server installation” on page 44.

See “Registering a detection server” on page 45.

Detection servers and remote indexers

Remote Indexing components should not reside on the same system that hosts a detection server. This restriction applies to two- and three-tier installations.

Indexing components are always installed with the Enforce Server, including on single-tier Symantec Data Loss Prevention installations.

The process of installing a remote indexer is similar to installing a detection server, except that you choose **Indexer** in the **Select Components** panel. See the *Symantec Data Loss Prevention Administration Guide* for detailed information on installing and using a remote indexer.

See “Installing a detection server” on page 40.

Detection server installation preparations

Before installing a detection server:

- You must install the Enforce Server (or a single-tier Symantec Data Loss Prevention installation) and import a solution pack before installing a detection server.
- Complete the preinstallation steps on the detection server system.
  See “Symantec Data Loss Prevention preinstallation steps” on page 19.
- Verify that the system is ready for detection server installation.
  See “Verifying that servers are ready for Symantec Data Loss Prevention installation” on page 21.
- Before you begin, make sure that you have access and permission to run the Symantec Data Loss Prevention installer software: `ProtectInstaller64_15.0.exe`.
- Before you begin, make sure that you have WinPcap. On the Internet, go to the following URL:
  http://www.winpcap.org
  See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for version requirements.

Note: The WinPcap software is only required for the Network Monitor Server. However, Symantec recommends that you install WinPcap no matter which type of detection server you plan to install and configure.

- Before you begin, make sure that you have Wireshark, available from www.wireshark.org. During the Wireshark installation process on Windows platforms, do not install a version of WinPcap lower than 4.1.2.
- Before you begin, make sure that you have Windows Services for UNIX (SFU) version 3.5 (`SFU35SEL_EN.exe`).

  SFU is required for a Network Discover Server to run a scan against a target on a UNIX machine. SFU can be downloaded from Microsoft.
- Symantec recommends that you disable any antivirus, pop-up locker, and registry-protection software before you begin the detection server installation process.

Preparing for Microsoft Rights Management file monitoring

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

Table 4-2 Microsoft Rights Management file monitoring prerequisites

RMS client	Requirements
Azure RMS	Install the RMS client, version 2.1, on the detection server.
AD RMS	■ Install the RMS client, version 2.1, on the detection server using a domain service user that is added to the AD RMS Super Users group. ■ Provide both the AD RMS Service User and the DLP Service User with Read and Execute permissions to access `ServerCertification.asmx`. Refer to the Microsoft Developer Network for additional details: https://msdn.microsoft.com/en-us/library/mt433203.aspx. ■ Add the detection server to the AD RMS server domain. ■ Run the detection server services using a domain user that is a member of the AD RMS Super Users group.

After you install the detection server, you enable RMS file detection. See "Enabling Microsoft Rights Management file monitoring" on page 43.

Installing a detection server

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

See "About detection servers" on page 36.

Note: The following instructions assume that the `ProtectInstaller64_15.0.exe` file has been copied into the `c:\temp` directory on the server computer.

To install a detection server

1. Make sure that installation preparations are complete.

   See "Detection server installation preparations" on page 38.

2. Log on (or remote logon) as Administrator to the computer that is intended for the 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 Symantec Data Loss Prevention installer (`ProtectInstaller64_15.0.exe`) from the Enforce Server to a local directory on the detection server.

   `ProtectInstaller64_15.0.exe` 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.
5. Click **Start > Run > Browse** to navigate to the folder where you copied the `ProtectInstaller64_15.0.exe` file.
6. Double-click `ProtectInstaller64_15.0.exe` to execute the file, and click **OK.**

   The installer files unpack, and the **Welcome** panel of the Installation Wizard appears.
7. Click **Next**.

   The **License Agreement** panel appears.
8. After reviewing the license agreement, select **I accept the agreement**, and click **Next**.

   The **Select Components** panel appears.
9. In the **Select Components** panel, select **Detection** and click **Next**.

10 In the **Hosted Network Prevent** panel, select the **Hosted Network Prevent** option only if you are installing a Network Prevent for Email or Network Prevent for Web server into a hosted environment, or to an environment that connects to the Enforce Server by a WAN. If you are installing a hosted Network Prevent server, you will also need to generate and install unique certificates to secure server communication.

See "About hosted Network Prevent deployments" on page 11.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.

11 In the **Select Destination Directory** panel, accept the default destination directory, or enter an alternate directory, and click **Next**. For example:

```
c:\SymantecDLP
```

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

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.

Note: Do not install Symantec Data Loss Prevention in a folder or path that includes spaces. For example, `c:\Program Files\SymantecDLP` is not a valid installation location.

---

12 In the **Select Start Menu Folder** panel, enter the Start Menu folder where you want the Symantec Data Loss Prevention shortcuts to appear.

The default is Symantec DLP.

13 Select one of the following options:

- **Create shortcuts for all users**
  The shortcuts are available in the same location for all users of the Enforce Server.
- **Don't create a Start Menu folder**
  The Symantec Data Loss Prevention shortcuts are not available from the Start menu.

14 In the **System Account** panel select one of the following options:

- **Create a new service user**
  Select this item if want to create a new service user. If you select this item you use a local service user to manage the detection server.
- **Use an existing service user**
  Select this item if you want to use an existing service user. If you select this item you can use a domain service user to manage the detection server. For example, if you want to use the RMS detection feature, you select this option.

15 Click Next.

16 In the **System Account** panel, create the Symantec Data Loss Prevention system account user name and password, and confirm the password. Then click **Next**.

This account is used to manage the Symantec Data Loss Prevention services.

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.

Note: To use the RMS detection feature, you must enable it after installing the detection server. See "Enabling Microsoft Rights Management file monitoring" on page 43.

The password you enter for the System Account must conform to the password policy of the server operating system. For example, the server on which you install Symantec Data Loss Prevention may require that all passwords include special characters.

The **Transport Configuration** panel appears.

17 Enter the following settings and then click **Next**.

- **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.
- **Network Interface** (bind address). Enter the detection server network interface to use to communicate with the Enforce Server. If there is only one network interface, leave this field blank.

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

18 Check the **Start Services** box, to start the Symantec Data Loss Prevention services and then Click **Finish**.

The services can also be started or stopped using the Windows Services utility.

Note that starting all of the services can take up to a minute. The installation program window may persist for a while, during the startup of the services.

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

20 Verify the detection server installation.

See “Verifying a detection server installation” on page 44.

21 Use the Enforce Server administration console to register the server with the Enforce Server.

During the server registration process, you select the type of detection server.

See “Registering a detection server” on page 45.

See “Verifying a detection server installation” on page 44.

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 the detection server have been completed. See “Preparing for Microsoft Rights Management file monitoring” on page 39.

Enabling RMS detection for Azure-managed RMS

For Azure RMS, complete the following on each detection server to enable RMS file monitoring:

1 Run the plugin: `Enable-Plugin.ps1`, which is located at located at `\\SymantecDLP\Protect\bin` on the Enforce Server.

```
powershell.exe -ExecutionPolicy RemoteSigned -File
"C:\SymantecDLP\Protect\plugins\contentextraction
\MicrosoftRightsManagementPlugin\Enable-Plugin.ps1"
```

2 Run the configuration utility `ConfigurationCreator.exe` to add the system user. Run the utility as the protect user.

Note: Enter all credentials accurately to ensure that the feature is enabled.

```
C:\SymantecDLP\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` at `\SymantecDLP\Protect\plugins\contentextraction\`:

- `rightsManagementConfiguration`
- `rightsManagementConfigurationProtection`

3 Restart each detection server to complete the process.

Note: You can confirm that Symantec Data Loss Prevention is monitoring RMS content by reviewing the `ContentExtractionHost_FileReader.log` file (located at *\SymantecDLP\Protect\Logs\debug*). Error messages that display for the `MicrosoftRightsManagementPlugin.cpp` item indicate that the plugin is not monitoring RMS content.

Enabling RMS detection for AD-managed RMS

For AD RMS, complete the following on each detection server to enable RMS file monitoring:

1 Run the plugin: `Enable-Plugin.ps1`, which is located at located at `\SymantecDLP\Protect\bin` on the Enforce Server.

```
powershell.exe -ExecutionPolicy RemoteSigned -File
"C:\SymantecDLP\Protect\plugins\contentextraction\
MicrosoftRightsManagementPlugin\Enable-Plugin.ps1"
```

2 Restart each detection server to complete the process.

Note: You can confirm that Symantec Data Loss Prevention is monitoring RMS content by reviewing the `ContentExtractionHost_FileReader.log` file (located at *\SymantecDLP\Protect\Logs\debug*). Error messages that display for the `MicrosoftRightsManagementPlugin.cpp` item indicate that the plugin is not monitoring RMS content.

Verifying a detection server installation

After installing a server, verify that it is correctly installed before you register it.

See "Installing a detection server" on page 40.

To verify a detection server installation

1. If you selected the option **Start Services**, then confirm that the `VontuMonitor` and `VontuUpdate` services are running.
2. If the Symantec Data Loss Prevention services do not start, check log files for possible issues (for example, connectivity, password, or database access issues).
   - The Symantec Data Loss Prevention installation log is `c:\SymantecDLP\.install4j\installation.log`
   - Symantec Data Loss Prevention operational logs are in `c:\SymantecDLP\Protect\logs`

Registering a detection server

Before registering a server, you must install and verify the server software.

See "Installing a detection server" on page 40.

See "Verifying a detection server installation" on page 44.

After the detection server is installed, use the Enforce Server administration console to register the detection server as the type of detection server you want.

To register a detection server

1. Log on to the Enforce Server as Administrator.
2. Go to **System > Servers > Overview**.

   The System Overview page appears.
3. Click **Add Server**.
4. Select the type of detection server to add and click **Next**.

   The following detection server options are available:
   - For Network Monitor Server select **Network Monitor.**
   - For Network Discover/Cloud Storage Discover Server select **Network Discover/Cloud Storage Discover.**
     If you want to install Network Protect, make sure you are licensed for Network Protect and select the **Network Discover** option. Network Protect provides additional protection features to Network Discover/Cloud Storage Discover.
   - For Network Prevent for Email Server select **Network Prevent for Email.**
   - For Network Prevent for Web Server select **Network Prevent for Web.**
   - For Endpoint Prevent and Endpoint Discover select **Endpoint Prevent.**
   - For Single-Tier Servers, select **Single Tier Monitor**.

See "About detection servers" on page 36.

The **Configure Server** screen appears.

5 Enter the General information. This information defines how the server communicates with the Enforce Server.

- In **Name**, enter a unique name for the detection server.
- In **Host**, enter the detection server's host name or IP address. For a single-tier installation, click the **Same as Enforce** check box to autofill the host information. For a **Single Tier Monitor**, the local host is pre-selected.
- In **Port**, enter the port number the detection server uses to communicate with the Enforce Server. If you chose the default port when you installed the detection server, then enter 8100. However, if you changed the default port, then enter the same port number here (it can be any port higher than 1024).

The additional configuration options displayed on the **Configure Server** page vary according to the type of server you selected.

6 Specify the remaining configuration options as appropriate.

See the *Symantec Data Loss Prevention Administration Guide* for details on how to configure each type of server.

7 Click **Save**.

The **Server Detail** screen for that server appears.

8 If necessary, click **Server Settings** or other configuration tabs to specify additional configuration parameters.

9 If necessary, restart the server by clicking **Recycle** on the **Server Detail** screen. Or you can start the Vontu services manually on the server itself.

See "About Symantec Data Loss Prevention services" on page 129.

10 To verify that the server was registered, return to the **System Overview** page. Verify that the detection server appears in the server list, and that the server status is **Running**.

11 To verify the type of certificates that the server uses, select **System > Servers > Alerts**. Examine the list of alerts to determine the type certificates that Symantec Data Loss Prevention servers use:

- If servers use the built-in certificate, the Enforce Server shows a warning event with code 2709: Using built-in certificate.
- If servers use unique, generated certificates, the Enforce Server shows an info event with code 2710: Using user generated certificate.

Registering the Single Tier Monitor

After you have installed Symantec Data Loss Prevention in single-tier mode, you can register and configure the Single Tier Monitor. To register the Single Tier Monitor, you add the server and configure its general settings. To configure the Single Tier Monitor, you configure the channels for each detection server type for which you have a license.

For more information about configuring and maintaining detection servers, see the *Symantec Data Loss Prevention Administration Guide*.

To register the Single Tier Monitor

1. Log on to the Enforce Server as Administrator.
2. Go to **System > Servers > Overview**.

   The **System Overview** page appears.
3. Click **Add Server**.

   The **Add Server** page appears.
4. Select **Single Tier Monitor**, then click **Next**.

   The **Configure Server** screen appears.
5. Enter the General information. This information defines how the server communicates with the Enforce Server.
   - In the **Name** field, enter a unique name for the detection server.
   - The **Host** field is already set to the local host address. You cannot change this setting.
   - In the **Port** field, enter the port number the detection server uses to communicate with the Enforce Server. By default, the port is set to 8100. If you want to use a different port number, enter any port number greater than 1024 here.
6. Specify the remaining configuration options as appropriate.

   See the *Symantec Data Loss Prevention Administration Guide* for details on how to configure the Single Tier Monitor.
7. After you have configured each detection channel, click **Save**.

   The **Server Detail** screen appears.
8. If necessary, click **Server Settings** or other configuration tabs to specify additional configuration parameters.
9. If necessary, restart the server by clicking **Recycle** on the **Server Detail** screen. Or you can start the Vontu services manually on the server itself.

   See "About Symantec Data Loss Prevention services" on page 129.

10 To verify that the server was registered, return to the System Overview page. Verify that the detection server appears in the server list, and that the server status is **Running**.

11 To verify the type of certificates that the server uses, select **System > Servers > Alerts**. Examine the list of alerts to determine the type certificates that Symantec Data Loss Prevention servers use:

- If servers use the built-in certificate, the Enforce Server shows a warning event with code 2709: Using built-in certificate.
- If servers use unique, generated certificates, the Enforce Server shows an info event with code 2710: Using user generated certificate.

Chapter 5

Configuring certificates for secure communications between Enforce and detection servers

This chapter includes the following topics:

About the sslkeytool utility and server certificates

Symantec Data Loss Prevention uses Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt all data that is transmitted between servers. Symantec Data Loss Prevention also uses the SSL/TLS protocol for mutual authentication between servers. Servers implement authentication by the mandatory use of client and server-side certificates. By default, connections between servers use a single, self-signed certificate that is embedded securely inside the Symantec Data Loss Prevention software. All Symantec Data Loss Prevention installations at all customer sites use this same certificate.

Symantec recommends that you replace the default certificate with unique, self-signed certificates for your organization's installation. You store a certificate on the Enforce Server,

and on each detection server that communicates with the Enforce Server. These certificates are generated with the sslkeytool utility.

Note: If you install a Network Prevent detection server in a hosted environment, you must generate unique certificates for your Symantec Data Loss Prevention servers. You cannot use the built-in certificate to communicate with a hosted Network Prevent server.

Symantec recommends that you create dedicated certificates for communication with your Symantec Data Loss Prevention servers. When you configure the Enforce Server to use a generated certificate, all detection servers in your installation must also use generated certificates. You cannot use the generated certificate with some detection servers and the built-in certificate with other servers. Single-tier deployments do not support generated certificates. You must use the built-in certificate with singler-tier deployments.

See "About sslkeytool command line options" on page 50.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.

See "Using sslkeytool to add new detection server certificates" on page 55.

See "About server security and SSL/TLS certificates" on page 112.

About sslkeytool command line options

The `sslKeyTool` is a command-line utility that generates a unique pair of SSL certificates (keystore files). The `sslKeyTool` utility is located in directory `\SymantecDLP\Protect\bin` directory (Windows) or `/opt/SymantecDLP/Protect/bin` (Linux). It must run under the Symantec Data Loss Prevention operating system user account which, by default, is "protect." Also, you must run the `sslKeyTool` utility directly on the Enforce Server computer.

Table 5-1 lists the command forms and options that are available for the `sslKeyTool` utility:

Table 5-1 sslKeyTool command forms and options

Command and options	Description
`sslKeyTool -genkey [-dir=<directory> -alias=<aliasFile>]`	You use this command form the first time you generate unique certificates for your Symantec Data Loss Prevention installation. This command generates two unique certificates (keystore files) by default: one for the Enforce Server and one for other detection servers. The optional `-dir` argument specifies the directory where the keystore files are placed. The optional `-alias` argument generates additional keystore files for each alias specified in the *aliasFile*. You can use the alias file to generate unique certificates for each detection server in your system (rather than using a same certificate on each detection server).
`sslKeyTool -list=<file>`	This command lists the content of the specified keystore file.
`sslKeyTool -alias=<aliasFile> -enforce=<enforceKeystoreFile> [-dir=<directory>]`	You use this command form to add new detection server certificates to an existing Symantec Data Loss Prevention installation. This command generates multiple certificate files for detection servers using the aliases you define in *aliasFile*. You must specify an existing Enforce Server keystore file to use when generating the new detection server keystore files. The optional `-dir` argument specifies the directory where the keystore files are placed. If you do not specify the `-dir` option, the Enforce Server keystore file must be in the current directory, and the monitor certificates will appear in the current directory. If you do specify the `-dir` argument, you must also place the Enforce Server keystore file in the specified directory.

Table 5-2 provides examples that demonstrate the usage of the `sslKeyTool` command forms and options.

Table 5-2 sslKeyTool examples

Example	Description
`sslkeytool -genkey`	This command generates two files: ■ `enforce.timestamp.sslKeyStore` ■ `monitor.timestamp.sslKeyStore` Unless you specified a different directory with the `-dir` argument, these two keystore files are created in the `bin` directory where the sslkeytool utility resides.
`sslkeytool -alias=Monitor.list.txt -enforce=enforce.date.sslkeystore`	Without the directory option `-dir`, the Enforce Server certificate must be in the current directory. The new detection server certificate(s) will be created in the current directory.
`sslkeytool -alias=Monitor.list.txt -enforce=enforce.date.sslkeystore -dir=C:\TEMP`	With the directory option `-dir=C:\TEMP`, the Enforce Server certificate must be in the `C:\TEMP` directory. The new detection server certificate(s) will be created in the `C:\TEMP` directory. **Note:** Use the absolute path for the `-dir` option unless the path is relative to the current directory.

See "About the sslkeytool utility and server certificates" on page 49.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.

See "Using sslkeytool to add new detection server certificates" on page 55.

See "About server security and SSL/TLS certificates" on page 112.

Using sslkeytool to generate new Enforce and detection server certificates

After installing Symantec Data Loss Prevention, use the `-genkey` argument with `sslKeyTool` to generate new certificates for the Enforce Server and detection servers. Symantec recommends that you replace the default certificate used to secure communication between servers with unique, self-signed certificates. The `-genkey` argument automatically generates two certificate files. You store one certificate on the Enforce Server, and the second certificate on each detection server. The optional `-alias` command lets you generate a unique certificate file for each detection server in your system. To use the `-alias` you must first create an alias file that lists the name of each alias create.

Note: The steps that follow are for generating unique certificates for the Enforce Server and detection servers at the same time. If you need to generate one or more detection server certificates after the Enforce Server certificate is generated, the procedure is different. See "Using sslkeytool to add new detection server certificates" on page 55.

To generate unique certificates for Symantec Data Loss Prevention servers

1. Log on to the Enforce Server computer using the "protect" user account you created during Symantec Data Loss Prevention installation.
2. From a command window, go to the directory where the `sslKeyTool` utility is stored:

   On Windows this directory is `c:\SymantecDLP\Protect\bin`.
3. If you want to create a dedicated certificate file for each detection server, first create a text file to list the alias names you want to create. Place each alias on a separate line. For example:

   ```
   net_monitor01
   protect01
   endpoint01
   smtp_prevent01
   web_prevent01
   ```

   Note: The `-genkey` argument automatically creates certificates for the "enforce" and "monitor" aliases. Do not add these aliases to your custom alias file.
4. Run the `sslkeytool` utility with the `-genkey` argument and optional `-dir` argument to specify the output directory. If you created a custom alias file, also specify the optional `-alias` argument, as in the following example:

   Windows:

   ```
   sslkeytool -genkey -alias=.\aliases.txt -dir=.\generated_keys
   ```

   This generates new certificates (keystore files) in the specified directory. Two files are automatically generated with the `-genkey` argument:

   - `enforce.`*`timestamp`*`.sslKeyStore`
   - `monitor.`*`timestamp`*`.sslKeyStore`

   The `sslkeytool` also generates individual files for any aliases that are defined in the alias file. For example:

   - net_monitor01.*timestamp*.sslKeyStore

- protect01.*timestamp*.sslKeyStore
- endpoint01.*timestamp*.sslKeyStore
- smtp_prevent01.*timestamp*.sslKeyStore
- web_prevent01.*timestamp*.sslKeyStore

5 Copy the certificate file whose name begins with `enforce` to the keystore directory on the Enforce Server.

On Windows the path is `c:\SymantecDLP\Protect\keystore`.

6 If you want to use the same certificate file with all detection servers, copy the certificate file whose name begins with `monitor` to the keystore directory of each detection server in your system.

On Windows the path is `c:\SymantecDLP\Protect\keystore`.

If you generated a unique certificate file for each detection server in your system, copy the appropriate certificate file to the `keystore` directory on each detection server computer.

7 Delete or secure any additional copies of the certificate files to prevent unauthorized access to the generated keys.

8 Restart the `VontuMonitorController` service on the Enforce Server and the `VontuMonitor` service on the detection servers.

When you install a Symantec Data Loss Prevention server, the installation program creates a default keystore in the `keystore` directory. When you copy a generated certificate file into this directory, the generated file overrides the default certificate. If you later remove the certificate file from the keystore directory, Symantec Data Loss Prevention reverts to the default keystore file embedded within the application. This behavior ensures that data traffic is always protected. Note, however, that you cannot use the built-in certificate with certain servers and a generated certificate with other servers. All servers in the Symantec Data Loss Prevention system must use either the built-in certificate or a custom certificate.

Note: If more than one keystore file is placed in the keystore directory, the server does not start.

See "Using sslkeytool to add new detection server certificates" on page 55.

See "About sslkeytool command line options" on page 50.

See "About the sslkeytool utility and server certificates" on page 49.

See "About server security and SSL/TLS certificates" on page 112.

Using sslkeytool to add new detection server certificates

Use `sslkeytool` with the `-alias` argument to generate new certificate files for an existing Symantec Data Loss Prevention deployment. When you use this command form, you must provide the current Enforce Server keystore file, so that `sslkeytool` can embed the Enforce Server certificate in the new detection server certificate files that you generate.

To generate new detection server certificates provides instructions for generating one or more new detection server certificates.

To generate new detection server certificates

1. Log on to the Enforce Server computer using the "protect" user account that you created during Symantec Data Loss Prevention installation.
2. From a command window, go to the bin directory where the `sslkeytool` utility is stored.

   On Windows the path is `c:\SymantecDLP\Protect\bin`.
3. Create a directory in which you will store the new detection server certificate files. For example:

   ```
   mkdir new_certificates
   ```
4. Copy the Enforce Server certificate file to the new directory. For example:

   Windows command:

   ```
   copy ..\keystore\enforce.Fri_Jun_12_11_24_20_PDT_2016.sslkeyStore
        .\new_certificates
   ```
5. Create a text file that lists the new server alias names that you want to create. Place each alias on a separate line. For example:

   ```
   network02
   smtp_prevent02
   ```

6 Run the `sslkeytool` utility with the `-alias` argument and `-dir` argument to specify the output directory. Also specify the name of the Enforce Server certificate file that you copied into the certificate directory. For example:

Windows command:

```
sslkeytool -alias=.\aliases.txt
  -enforce=enforce.Fri_Jun_10_11_24_20_PDT_2016.sslkeyStore
  -dir=.\new_certificates
```

This generates a new certificate file for each alias, and stores the new files in the specified directory. Each certificate file also includes the Enforce Server certificate from the Enforce Server keystore that you specify.

7 Copy each new certificate file to the keystore directory on the appropriate detection server computer.

On Windows the path is `c:\SymantecDLP\Protect\keystore`.

Note: After creating a new certificate for a detection server (`monitor.date.sslkeystore`), the Enforce Server certificate file (`enforce.date.sslkeystore`) is updated with the context of each new detection server. You need to copy and replace the updated Enforce Server certificate to the keystore directory and repeat the process for each new detection server certificate you generate.

---

8 Delete or secure any additional copies of the certificate files to prevent unauthorized access to the generated keys.

9 Restart the `VontuMonitor` service on each detection server to use the new certificate file.

Verifying server certificate usage

Symantec Data Loss Prevention uses system events to indicate whether servers are using the built-in certificate or user-generated certificates to secure communication. If servers use the default, built-in certificate, Symantec Data Loss Prevention generates a warning event. If servers use generated certificates, Symantec Data Loss Prevention generates an info event.

Symantec recommends that you use generated certificates, rather than the built-in certificate, for added security.

If you install Network Prevent to a hosted environment, you cannot use the built-in certificate and you must generate and use unique certificates for the Enforce Server and detection servers.

To determine the type of certificates that Symantec Data Loss Prevention uses

1. Start the Enforce Server or restart the `VontuMonitorController` service on the Enforce Server computer.
2. Start each detection server or restart the `VontuMonitor` service on each detection server computer.
3. Log in to the Enforce Server administration console.
4. Select **System > Servers > Alerts**.
5. Check the list of alerts to determine the type certificates that Symantec Data Loss Prevention servers use:
   - If servers use the built-in certificate, the Enforce Server shows a warning event with code 2709: Using built-in certificate.
   - If servers use unique, generated certificates, the Enforce Server shows an info event with code 2710: Using user generated certificate.

Chapter 6

Installing the domain controller agent to identify users in incidents

This chapter includes the following topics:

About the domain controller agent

You can identify specific users in Symantec Data Loss Prevention Network Prevent for Web incidents by installing the Symantec Data Loss Prevention domain controller agent. The domain controller agent enables you to resolve user names from IPv4 address and associates the IP addresses in those incidents with user names in the User Risk Summary. The domain controller agent queries Windows Events in the Microsoft Active Directory security event log of the domain controller. Symantec Data Loss Prevention associates these Windows Events with user data in your database. See the "User Risk Summary" section in the *Symantec Data Loss Prevention Administration Guide*.

The domain controller agent runs only on Windows Server 2008 and later operating systems. For specific supported version information, see the *Symantec Data Loss Prevention System*

Requirements and Compatibility Guide. Symantec recommends installing the domain controller agent on a dedicated server. The domain controller agent can connect to multiple domain controllers.

The following User Identification configurations are not supported:

- One domain controller agent to multiple Enforce Servers
- Linux domain controllers
- Domain controller agents installed on endpoints

Domain controller agent installation prerequisites

Before you install the domain controller agent, take the following steps:

- Add the domain controller agent host server to the domain before installing the server.
- Install the domain controller agent host server using domain administrator credentials.
- Ensure that the domain controller agent host server can communicate with your Windows Active Directory domain controller host and the Enforce Server host.
- Note the user name and password for logging on to the domain controller server.
- Note the domain controller fully qualified domain name (FQDN).
- Create a dedicated Enforce Server account for the domain controller agent. This account should have privileges for accessing the web service and database tables.
  For detailed information about creating an Enforce Server account, see the *Symantec Data Loss Prevention Administration Guide*.
- Note the user name and password for logging on to the Enforce Server.
- Note the Enforce Server fully qualified domain name (FQDN).
- Note the TCP HTTPS port number you want to use to connect to the Enforce Server. By default, the domain controller agent connects to port 443 on Windows systems. To connect the domain controller agent to a Enforce Server on the Linux platform, use port 8443 or any other appropriate Linux port.
- Optional: If you want to use certificate authentication, note the path to your Enforce Server certificate and the path to the CA root certificate.

Installing the domain controller agent

To install the domain controller agent, follow this procedure:

To install the domain controller agent

1. Copy the `symc_dcagent.msi` Windows Installer file from *DLPDownloadHome*`\DLP\15.0\Domain_Controller_Agent_Installer\` to your domain controller agent host server.
2. Run the `symc_dcagent.msi` Windows Installer file as an Administrator.

   The **Vontu Domain Controller Agent Setup** Wizard appears.
3. Read the end-user license agreement and accept the terms.
4. Click **Next**.

   The **Destination Folder** panel appears.
5. Enter the destination folder for the domain controller agent installation. By default, the domain controller agent installation folder is `C:\SymantecDLP\DC Agent`.
6. Click **Next**.

   The **Domain Controller Configuration** panel appears.
7. Enter the fully qualified domain name (FQDN) of your domain controller.
8. Click **Next**.

   The **DC Agent Service Configuration** panel appears.
9. Enter the logon (DOMAIN\USERNAME) and password for the Active Directory user that the domain controller agent uses to query the domain controller.
10. Click **Next**.

    The **Symantec DLP Enforce Server Configuration** panel appears.
11. Enter the following information:
    - The Enforce Server host name
    - The Enforce Server port
    - The logon name for the domain controller agent Enforce Server account
    - The password for the domain controller agent Enforce Server account
    - Optional: If you choose to use certificate authentication, select **Use a certificate to authenticate?**, then enter the path to the Enforce Server certificate and the CA root certificate, both located on your Enforce Server.
12. Click **Next**.

    The **DC Agent Communication Configuration** panel appears.
13. Enter the following information:

- Communication Interval: This value specifies how often the domain controller agent connects to the domain controller to collect events, in seconds. The default communication interval is 1 hour (3600 seconds).
- Lookback Time: This value specifies the time frame for which the domain controller collects events from the domain controller, in seconds. The default lookback time is 12 hours (43200 seconds).

14 Click **Next**.

The **Ready to Install Vontu Domain Controller Agent** panel appears.

15 Click **Next**.

The **Installing Vontu Domain Controller Agent** panel appears and displays a progress bar.

16 Click **Finish** to complete the installation of the domain controller agent.

Domain controller agent post-installation tasks

To confirm the installation, check that the domain controller agent (DC Agent) service is running. If the service is not running, see the troubleshooting section in this chapter.

See “Troubleshooting the domain controller agent” on page 63.

After you have installed the domain controller agent, the following parameters can be set up on the **System > Incident Data > User Identification** page in the Enforce Server administration console:

- Set the User data retention schedule in days
  Set the Domain controller warning in days
- Set the mapping Schedule
- View status of installed domain controllers

See "Identifying users in web incidents" in the *Symantec Data Loss Prevention Administration Guide* for more information.

Excluding an IP address or IP range from event collection

You can add an optional list of IP addresses or IP ranges to be excluded from event collection. Symantec recommends excluding the domain controller IP from event collection.

To exclude an IP address or IP range from event collection

1. Open the `SymantecDLP\DC Agent\DCAgentConfig.properties` file in a text editor.
2. Enter an IP address or IP range in CIDR notation for the EXCLUDED_EVENT_IPS parameter. For example:

   ```
   EXCLUDED_EVENT_IPS=1.2.3.4, 5.6.7.0/24, 8.9.10.11, 12.0.0.0/8
   ```

3. Save and close the `DCAgentConfig.properties` file.
4. Restart the DC Agent service to apply your changes.

Updating configuration settings after installation

You can edit your domain controller agent settings in the `SymantecDLP\DC Agent\DCAgentConfig.properties` file. After editing this file, restart the DC Agent service to apply your updated settings.

To update domain controller agent configuration settings

1. Open the `SymantecDLP\DC Agent\DCAgentConfig.properties` file in a text editor.
2. Edit the parameters for the configuration setting you want to change:
   - DC_HOSTNAME: Specifies the domain controller host names in the format DC_HOSTNAME=MACHINE1;MACHINE2;MACHINE3. Separate multiple host names with semicolons.
   - DC_LOGIN_TIMEOUT: Specifies the span of time that a user login event from a domain controller lasts. For example, if a login occurs at 1:00, and DC_LOGIN_TIMEOUT=90, the event forms a range from 1:00-2:30. Login timeouts are matched to the DC_HOSTNAME property list by order. Any Domain Controllers with unspecified login timeouts will be assigned the default value of 90 minutes.
   - EVENTS_BUFFER_SIZE: Specifies the number of events in the domain controller agent buffer. The default value is 1024.
   - ENFORCE_HOSTNAME: Specifies the name of the Enforce Server host.
   - ENFORCE_PORT: Specifies the port number through which the domain controller agent connects to the Enforce Server.
   - SSL_CA_ROOT_CERTIFICATE: Specifies the file system path to the CA root certificate.
   - SSL_HOST_CERTIFICATE: Specifies the file system path to the Enforce Server certificate.
   - HTTP_CONNECT_TIMEOUT: Specifies the connection timeout value. The default timeout value is 300 seconds.
     HTTP_SESSION_TIMEOUT: Specifies the session timeout value. The default session timeout value is 0 (the session never times out).

- COMMUNICATION_INTERVAL: Specifies how often the domain controller agent connects to the domain controller to collect events, in seconds. The default communication interval is 1 hour (3600 seconds).
- HTTP_POST_MAX_EVENTS: Specifies the maximum number of events to collect and post in a single HTTP request. The default value is 1024.
- LOG_CONFIGURATION_FILE=DCAgentLogging.properties: Place this log configuration file in the DCAgent installation directory.

3 Save and close the `DCAgentConfig.properties` file.

4 Restart the DC Agent service to apply your configuration changes.

Updating the Enforce Server logon for the domain controller agent

You can update the Enforce Server logon credential for the domain controller agent in the Credential Manager on the domain controller agent host server.

Updating the Enforce Server logon for the domain controller agent

1 Log on to the domain controller agent host server as the Service Logon user.

2 In the **Credential Manager** (**Control Panel > User Accounts > Credential Manager**), edit the generic credential for the Enforce Server.

3 Click **Save**.

Troubleshooting the domain controller agent

User Identification is disabled by default. Mapping is enabled only when you configure a mapping schedule at **System > Incident Data> User Identification**. If you have trouble with the domain controller agent, check the following items.

Table 6-1 Troubleshooting the domain controller agent

Problem	Solution
There are no entries in the **Domain Controllers** list.	User identification is disabled by default. Go to **System > Incident Data > User Identification** and set a mapping schedule.

Table 6-1 Troubleshooting the domain controller agent *(continued)*

Problem	Solution
The domain controller agent service does not start	Check the domain controller log at **System > Incident Data > User Identification** page. If there are no entries on the list, verify that the files were installed correctly and that the domain controller agent log-on user account has permission to run the service. Start the service manually. If there are errors in the log, verify that the log-on user for the Enforce Server has the correct credentials and switch to TRACE to collect the trace log.
The IPU tables in the database have no events	Check the Enforce Server logs and verify that the log-on user for the Enforce Server has the correct credentials. Verify Windows vault entries for the service log-on user. If you use certificate authentication, verify the private key in your Enforce Server certificate store and the public key in the domain controller agent installation directory.

Uninstalling the domain controller agent

You can uninstall the domain controller agent from Windows (**Control Panel > Programs > Programs and Features > Uninstall** a program), or by running the `symc_dcagent.msi` Window Installer file again and selecting **Remove**.

Chapter 7

Performing a single-tier installation

This chapter includes the following topics:

Installing a single-tier server

Before performing a single-tier installation:

- Complete the preinstallation steps.
  See "Symantec Data Loss Prevention preinstallation steps" on page 19.
- Verify that the system is ready for installation.
  See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 21.
- For single-tier Symantec Data Loss Prevention installations, the Oracle software is installed on the Enforce Server. You must install the Oracle software and Symantec Data Loss Prevention database before installing the single-tier server.
  See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.
- Before you begin, make sure that you have access and permission to run the Symantec Data Loss Prevention installer software: `ProtectInstaller64_15.0.exe`.

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

Note: The following instructions assume that the `ProtectInstaller64_15.0.exe` file, license file, and solution pack file have been copied into the `c:\temp` directory on the Enforce Server.

To install the single-tier server

1. Log on (or remote log on) as Administrator to the computer that is intended for the Symantec Data Loss Prevention single-tier installation.
2. Install WinPcap on the system before installing 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 (`ProtectInstaller64_15.0.exe`) from *`DLPDownloadHome`* to a local directory on the Enforce Server computer.
4. Click **Start > Run > Browse** to navigate to the folder where you copied the `ProtectInstaller_15.0.exe` file.
5. Double-click `ProtectInstaller_15.0.exe` to execute the file, and click **OK.**
6. The installer files unpack, and a welcome notice appears. Click **Next**.
7. In the **License Agreement** panel, select **I accept the agreement**, and click **Next**.
8. In the **Select Components** panel, select the **Single Tier** installation option, and click **Next**.
9. In the **License File** panel, browse to the directory containing your license file. Select the license file, and click **Next**.

   License files have names in the format *`name`*`.slf`.

10 In the **Select Destination Directory** panel, accept the Symantec Data Loss Prevention default destination directory and click **Next**.

```
c:\SymantecDLP
```

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.

Note: Do not install Symantec Data Loss Prevention in a folder or path that includes spaces. For example, `c:\Program Files\SymantecDLP` is not a valid installation location.

---

11 In the **Select Start Menu Folder** panel, enter the Start Menu folder where you want the Symantec Data Loss Prevention shortcuts to appear.

12 Select one of the following options and then click **Next**:

- **Create shortcuts for all users**
  The shortcuts are available in the same location for all users of the Enforce Server.
- **Don't create a Start Menu folder**
  The Symantec Data Loss Prevention shortcuts are not available from the Start menu.

13 In the **System Account** panel, create the Symantec Data Loss Prevention system account user name and password and confirm the password. Then click **Next**.

This account is used to manage Symantec Data Loss Prevention services. The password you enter for the System Account must conform to the password policy of the server operating system. For example, the server may require all passwords to include special characters.

14 In the **Transport Configuration** panel, accept the default port number (8100) on which the detection server should accept connections from the Enforce Server. You can change this default to any port higher than port 1024. Click **Next**.

15 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**.

16 In the **Oracle Database User Configuration** panel, enter the Symantec Data Loss Prevention database user name and password, confirm the password, and enter the database SID (typically “protect”). Then click **Next**.

See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.

If your Oracle database is not the required version, a warning notice appears. You can click **OK** to continue the installation and upgrade the Oracle database at a later time.

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 In the **Initialize DLP Database** panel, select one of the following options:

- For a new Symantec Data Loss Prevention installation, select the **Initialize Enforce Data** option.
  You can also selection this option if you are reinstalling and want to overwrite the existing Enforce schema and all data. Note that this action cannot be undone. If this check box is selected, the data in your existing Symantec Data Loss Prevention database is destroyed after you click **Next**.
- Clear the **Initialize Enforce Data** check box if you want to perform a recovery operation. Clearing the check box skips the database initialization process. If you choose skip the database initialization, you will need to specify the unique `CryptoMasterKey.properties` file for the existing database that you want to use.

19 In the **Single Sign On Option** panel, select the sign-on option that you want to use for accessing the Enforce Server administration console, then click **Next**:

Option	Description
Certificate Authentication	Select this option if you want users to automatically log on to the Enforce Server administration console using client certificates that are generated by your public key infrastructure (PKI). If you choose certificate authentication, you will need to import the certificate authority (CA) certificates required to validate users' client certificates. You will also need to create Enforce Server user accounts to map common name (CN) values in certificates to Symantec Data Loss Prevention roles. See the *Symantec Data Loss Prevention Administration Guide* for more information.
Password Authentication Only	Select **Password Authentication Only** if you want users to log onto the Enforce Server administration console using passwords entered at the sign-on page.

Note: If you are unsure of which sign on mechanism to use, select **None** to use the forms-based sign-on mechanism. Forms-based sign-on with password authentication is the default mechanism used in previous versions of Symantec Data Loss Prevention. You can choose to configure certificate authentication after you complete the installation, using instructions in the *Symantec Data Loss Prevention Administration Guide*.

---

20 If you selected **None** as your log on option, skip this step.

In the **Import Certificates** panel, select options for certificate authentication, then click **Next**:

Option	Description
Import Certificates **Select Certificate Directory**	Select **Import Certificates** if you want to import certificate authority (CA) certificates during the Enforce Server installation. CA certificates are required to validate client certificates when you choose **Certificate Authentication** sign on. If the necessary CA certificates are available on the Enforce Server computer, select **Import Certificates** and click **Browse** to navigate to the directory where the `.cer` files are located. Uncheck **Import Certificates** if the necessary certificates are not available on the Enforce Server computer, or if you do not want to import certificates at this time. You can import the required certificates after installation using instructions in the *Symantec Data Loss Prevention Administration Guide*.
Allow Form Based Authentication	Select this option if you want to support password authentication with forms-based sign-on in addition to single sign-on with certificate authentication. Symantec recommends that you select this as a backup option while you configure and test certificate authentication with your PKI. You can disable password authentication and forms-based sign-on after you have validated that certificate authentication is correctly configured for your system.

21 If you chose to initialize the Enforce Server database, skip this step.

If you chose to re-use an existing Enforce Server database, the installer displays the **Key Ignition Configuration** panel. Click **Browse** and navigate to select the unique `CryptoMasterKey.properties` file that was used to encrypt the database.

Note: 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 you do not have the `CryptoMasterKey.properties` file for the existing Enforce Server database, contact Symantec Technical Support to recover the file.

Click **Next** to continue the installation.

22 If you chose to re-use an existing Enforce Server database, skip this step.

In the **Administrator Credentials** panel, specify information according to the sign-on option that you selected and click **Next**:

Option	Description
Password **Re-enter Password**	If you chose an option to support password authentication with forms-based log on, enter a password for the Enforce Server Administrator account in both the **Password** and **Re-enter Password** fields. The Administrator password must contain a minimum of eight characters. You can change the Administrator password from the Enforce Server administration console at any time. **Note:** These fields are not displayed if you selected **Certificate Authentication** but you did not select **Allow Form Based Authentication**. In this case, you must log on to the Enforce Server administration console using a client certificate that contains the administrator's common name value.
Common Name (CN)	If you chose to support certificate authentication, enter the Common Name (CN) value that corresponds to the Enforce Server Administrator user. The Enforce Server assigns administrator privileges to the user who logs on with a client certificate that contains this CN value. **Note:** This field is displayed only if you selected **Certificate Authentication**.

23 Click **Next**.

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

24 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.

25 Click **Next**.

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

26 Confirm your participation in the Symantec Data Loss Prevention Supportability Telemetry program, and provide the appropriate information.

The Symantec Data Loss Prevention Supportability Telemetry Program can significantly improve the quality of Symantec Data Loss Prevention. For more information, click the Supportability and Telemetry Program Details link.

27 Click **Next**.

The installation process begins. After the Installation Wizard extracts the files, it connects to the database using the name and password that you entered earlier. The wizard then creates the database tables. If any problems with the database are discovered, a notification message displays.

The **Installing** panel appears, and displays a progress bar.

28 Select the **Start Services** check box to start the Symantec Data Loss Prevention services after the completion notice displays.

The services can also be started or stopped using the Windows Services utility.

29 Click **Finish**.

Starting all of the services can take up to a minute. The installation program window may persist for a while, during the startup of the services. After a successful installation, a completion notice displays.

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

See "Verifying a single-tier installation" on page 74.

31 You must import a Symantec Data Loss Prevention solution pack immediately after installing and verifying the single-tier server, and before changing any single-tier server configurations.

See "About Symantec Data Loss Prevention solution packs" on page 32.

32 After importing a solution pack, register the detection server component of the single-tier installation.

See "Registering a detection server" on page 45.

See "Registering the Single Tier Monitor" on page 47.

33 Back up the unique `CryptoMasterKey.properties` file for your installation and store the file in a safe place. This file is required for Symantec Data Loss Prevention to encrypt and decrypt the Enforce Server database.

Note: 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.

Verifying a single-tier installation

After installing Symantec Data Loss Prevention on a single-tier system, verify that it is operating correctly before importing a solution pack.

To verify a single-tier installation

1 If you selected the option **Start Services**, then confirm that all of the Symantec Data Loss Prevention Services are running under the System Account user name that you specified during installation.

Note that on Windows platforms, all services run the System Account user name except for the `VontuUpdate` services, which run *username*_update.

Symantec Data Loss Prevention includes the following services:

- `VontuManager`
- `VontuIncidentPersister`
- `VontuNotifier`
- `VontuUpdate`
- `VontuMonitor`
- `VontuMonitorController`

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

- The Symantec Data Loss Prevention installation log is in `c:\SymantecDLP\.install4j\installation.log`
- Symantec Data Loss Prevention operational logs are in `c:\SymantecDLP\Protect\logs`
- Oracle logs can be found in `c:\app\Administrator\admin\protect` 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.

Once you have verified the Enforce Server installation, you can log on to the Enforce Server to view the administration console.

See the *Symantec Data Loss Prevention Administration Guide* for information about logging on to, and using, the Enforce Server administration console.

You must import a Symantec Data Loss Prevention solution pack immediately after installing and verifying the single-tier server, and before changing any single-tier server configurations.

See "About Symantec Data Loss Prevention solution packs" on page 32.

After importing a solution pack, register a detection server.

See "Registering a detection server" on page 45.

See "Registering the Single Tier Monitor" on page 47.

Policy authoring considerations

For Single Server deployments, all policies are grouped in the **Default Policy Group**. Therefore, all policies will apply to every channel that you have configured. Take this into consideration when authoring your policies to avoid poor performance on your Single Server deployment.

For more information about policy authoring and policy groups, see the *Symantec Data Loss Prevention Administration Guide*.

About migrating to a two-tier deployment

As your Symantec Data Loss Prevention deployment grows, you may need to migrate your Single Server deployment to a two-tier deployment. A two-tier deployment is one in which the Oracle database and Enforce Server remain on one server, while you deploy individual detection servers for each detection type you have configured in your Single-tier Detection Server. The migration process preserves all of your existing policies, incidents, incident history, and Discover targets.

Migrating to a two-tier deployment is irreversible. You cannot migrate back to a Single Server deployment from a two-tier deployment.

For more information about two-tier installations, see the *Symantec Data Loss Prevention Installation Guide*.

To migrate to a two-tier deployment

1. Log on to the Enforce Server as Administrator.
2. Go to **System > Servers > Overview**.

   The **System Overview** page appears.
3. Click **Add Server**.

   The **Add Server** page appears.
4. Register and configure a new detection server for each detection type which you have a license. Each server requires its own dedicated hardware.

   For complete information about registering detection servers, see the *Symantec Data Loss Prevention Installation Guide*.

   For complete information about configuring detection servers, see the *Symantec Data Loss Prevention Administration Guide*
5. After you have registered and configured each detection server, remove the configuration from each tab on the **System > Servers Overview > Configure Server** page for the corresponding channel or channels on your Single Tier Monitor.
6. After you have deployed a new detection server for each of your detection server licenses, go to **System > Servers > Overview** and remove the Single Tier Monitor.

Chapter 8

Installing Symantec DLP Agents

This chapter includes the following topics:

DLP Agent installation overview

The following section describes the process to install DLP Agents.

Note: Before you begin the Symantec DLP Agent installation process, confirm that you have installed and configured an Endpoint Server. See “Detection server installation preparations” on page 38.

See “About Endpoint Server redundancy” on page 84.

Table 8-1 Agent installation steps

Step	Action	More information
1	Create the agent installation package. You create the agent installation package using the Enforce Server administration console.	See "About secure communications between DLP Agents and Endpoint Servers" on page 78.
2	Prepare endpoints for the installation. You prepare endpoints by completing the following: ■ Update settings on security software ■ Change the command prompt to run in elevated mode on the Windows endpoint on which to execute the installation. ■ Consider how to best set up Endpoint Servers to manage DLP Agents.	See "Identify security applications running on endpoints" on page 84. See "Using the Elevated Command Prompt with Windows" on page 85. See "About Endpoint Server redundancy" on page 84.
3	Install agents. You install agents to Windows and Mac endpoints depending on your implementation.	See "Process to install the DLP Agent on Windows" on page 86. See "Process to install the DLP Agent on Mac" on page 93.

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 83.

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 79.

Generating agent installation packages

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

See "About secure communications between DLP Agents and Endpoint Servers" on page 78.

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

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

Note: Before you start generating the agent installation packages, confirm that the agent installer has been copied to the Enforce Server local file system. See "Symantec Data Loss Prevention preinstallation steps" on page 19.

Table 8-2 provides instructions for generating agent installation packages. The instructions assume that you have deployed an Endpoint Server.

Table 8-2 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.
2	Select one or more DLP Agent installation files.	Browse to the folder on the Enforce Server where you copied the agent installer files: **Windows 64-bit**: `AgentInstall64_15_0.msi` **Windows 32-bit**: `AgentInstall_15_0.msi` **Mac 64-bit**: `AgentInstall_15_0.pkg` See "Symantec Data Loss Prevention preinstallation steps" on page 19.
3	Select the agent version.	Select an item in the **Select the agent version** list that matches the agent installer files you selected. You must select 32- and 64-bit installation files that match the agent version you selected. For example, selecting a version 14.6 32-bit and a version 15.0 64-bit installation file while selecting **Version 15.0** in the list is unsupported. Selecting mis-matched versions prevents agents from installing on endpoints.

Table 8-2 Generating the agent installation package *(continued)*

Step	Action	Description
4	Enter the server host name.	Typically you enter the common name (CN) of the Endpoint Server host, or you can enter the IP address of the server. Be consistent with the type of identifier you use (CN or IP). If you used the CN for the Endpoint Server when deploying it, use the same CN for the agent package. If you used an IP address to identify the Endpoint Server, use the same IP address for the agent package. Alternatively, you can enter the CN or IP address of a load balancer server.
5	Enter the port number for the server.	The default port is 10443. Typically you do not need to change the default port unless it is already in use or intended for use by another process on the server host.
6	Add additional servers (optional).	Click the plus sign icon 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. See "About Endpoint Server redundancy" on page 84.
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. See "About agent password management" on page 109.
8	Re-enter the Endpoint tools password.	The system validates that the passwords match and displays a message if they do not.

Table 8-2 Generating the agent installation package *(continued)*

Step	Action	Description
9	Enter the target directory for the agent installation (Windows only).	The default installation directory for Windows 32- and 64-bit agents is `%PROGRAMFILES%\Manufacturer\Endpoint Agent`. Change the default path if you want to install the Windows agent to a different location on the endpoint host. You can only install the DLP Agent to an ASCII directory using English characters. Using non-English characters can prevent the DLP Agent from starting and from monitoring data in some scenarios. **Note:** Include the drive letter if you plan to change the default directory. For example, use `C:\Endpoint Agent`. Not including a drive letter causes the agent installation to fail. The target directory for the Mac agent is set by default.
10	Enter the uninstall password (optional, Windows only).	The agent uninstall password is supported for Windows agents. The uninstall password is a tamper-proof mechanism that requires a password to uninstall the DLP Agent. The password is encrypted and stored in a file on the Enforce Server. You should store this password in a secure format of your own so that it can be retrieved if forgotten. See "About uninstallation passwords" on page 108. See "Removing a DLP Agent from a Mac endpoint" on page 138. After installing agents, you can change the password on the **Agent Password Management** screen. See "About agent password management" on page 109.
11	Re-enter the uninstall password.	The system validates that the passwords match and displays a message if they do not.
12	Click **Generate Installer Packages**.	This action generates the agent installer package for each platform that you selected in step 3. If you generate more than one package the generation process may take a few minutes.

Table 8-2 Generating the agent installation package *(continued)*

Step	Action	Description

13	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.
		
		If you generated a single agent package, the zip file is named one of the following corresponding to the agent installer you uploaded:
		
		`AgentInstaller_Win64.zip`
		
		`AgentInstaller_Win32.zip`
		
		`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 82.

14	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. See "DLP Agent installation overview" on page 77.

Agent installation package contents

You generate the agent installation package for Windows and Mac agents at the **System > Agents > Agent Packaging** screen.

See "Generating agent installation packages" on page 79.

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

See "DLP Agent installation overview" on page 77.

Table 8-3 `AgentInstaller_Win32.zip` and `AgentInstaller_Win64.zip` installation package contents

File name	Description
`AgentInstall_15_0.msi` or `AgentInstall64_15_0.msi`	Windows agent installer

Table 8-3 `AgentInstaller_Win32.zip` and `AgentInstaller_Win64.zip` installation package contents *(continued)*

File name	Description
`endoint_cert.pem`	Agent certificate and encryption keys See "Working with endpoint certificates" on page 83.
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`install_agent.bat`	Use to install the agent silently
`upgrade_agent.bat`	Use to upgrade the agent
`PackageGenerationManifest.mf`	Package metadata

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

See "DLP Agent installation overview" on page 77.

Table 8-4 `AgentInstaller_Mac64.zip` installation package contents

File	Description
`AgentInstall_15_0.pkg`	Mac agent installer
`AgentInstall.plist`	Mac agent installation properties configuration file
`create_package`	Use to generate the installation package for macOS. You can use this package to install agents manually or using deployment tools like Apple Remote Desktop (ARD).
`endoint_cert.pem`	Agent certificate and encryption keys See "Working with endpoint certificates" on page 83.
`endpoint_priv.pem`	
`endpoint_truststore.pem`	
`Install_Readme.rtf`	Provides installation steps
`PackageGenerationManifest.mf`	Package metadata

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 78.

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 79.

Identify security applications running on endpoints

Before you install the Symantec DLP Agent, identify all security applications that run on your endpoints. Configure those applications to allow the Symantec DLP Agents to function fully. Some applications generate alerts when they detect the installation or initial launch of a Symantec DLP Agent. Such alerts reveal the presence of Symantec DLP Agents and they sometimes let users block the Symantec DLP Agent entirely.

Note: See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about configuring third-party software to work with the Symantec DLP Agent.

Check the following applications:

- Antivirus software
- Firewall software

Make sure that your antivirus software and firewall software recognize the Symantec DLP Agents as legitimate programs.

About Endpoint Server redundancy

You can configure the DLP Agent to connect to multiple Endpoint Servers. Endpoint Servers can be connected using a load balancer. Multiple Endpoint Servers enable incidents and events to be sent to the Enforce Server in a timely way if an Endpoint Server becomes unavailable. For example, assume that an Endpoint Server becomes unavailable because of a network partition. The DLP Agent, after a specified amount of time, connects to another Endpoint Server to transmit the incidents and events that it has stored. The Symantec DLP Agent makes a best effort to fail over to a different Endpoint Server only when the current Endpoint Server is unavailable. If the original Endpoint Server is unavailable, the agent attempts

to connect to another Endpoint Server in the configured list. By default, the DLP Agent tries to reconnect to the original Endpoint Server for 60 minutes before it connects to another Endpoint Server. In a load-balanced Endpoint Server environment, the connection interval is managed by the load balancer.

When a DLP Agent connects to a new Endpoint Server, it downloads the policies from that Endpoint Server. It then immediately begins to apply the new policies. To ensure consistent incident detection after a failover, maintain the same policies on all Endpoint Servers to which the DLP Agent may connect.

For Endpoint Discover monitoring, if a failover occurs during a scan, the initial Endpoint Discover scan is aborted. The DLP Agent downloads the Endpoint Discover scan configuration and policies from the failover Endpoint Server and immediately runs a new scan. The new scan runs only if there is an active Endpoint Discover scan configured on the failover Endpoint Server.

You must specify the list of Endpoint Servers when you install the DLP Agents. The procedure for adding a list of Endpoint Servers appears under each method of installation. You can specify either IP addresses or host names with the associated port numbers. If you specify a host name, the DLP Agent performs a DNS lookup to get a set of IP addresses. It then connects to each IP address. Using host names and DNS lookup lets you make dynamic configuration changes instead of relying on a static install-time list of stated IP addresses.

Using the Elevated Command Prompt with Windows

If you install agents on endpoints that run Windows 7/8/8.1, you must run the command prompt in **Elevated Command Prompt** mode.

To initiate the Elevated Command Prompt mode on Windows 7

1. Click the **Start** menu.
2. In the **Search programs and files** field, enter **command prompt**.

   The **Command Prompt** program appears in the results list.
3. Hold the Shift key and right-click the **Command Prompt** entry in the results list. Select either **Run as Administrator** or **Run as different user**.
4. If you selected **Run as different user**, enter the credentials for a user that has administrator privileges.

To initiate the Elevated Command Prompt mode on Windows 8/8.1

1. Display the Command Prompt.
   - In Desktop mode, right-click on the Windows icon and select **Command Prompt (Admin)**, then click the **Start** menu.

- In Metro mode, enter **cmd** in the **Search programs and files** field.

2 Hold the Shift key and right-click **Command Prompt** in the results list.

3 Select **Run as Administrator**.

Process to install the DLP Agent on Windows

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

Note: If you plan to install DLP Agents running Windows 8 or Windows 8.1, verify that Admin Security mode is set to Disabled on the administrator account. This setting allows administrators to complete tasks such as running endpoint tools and installing agents.

Before you install DLP Agents on Windows endpoints, confirm that you have completed prerequisite steps. See "DLP Agent installation overview" on page 77.

Table 8-5 Process to install agents on Windows endpoints

Step	Action	Additional information
1	Install an agent manually. Install a single agent to test the configuration or to create a test scenario.	See "Installing the DLP Agent for Windows manually" on page 86.
2	Install the agents using your SMS. You install agents in this method to install many agents at one time.	See "Installing DLP Agents for Windows silently" on page 87.
3	Confirm that the agents are running.	See "Confirming that the Windows agent is running" on page 91.
4	(Optional) Review the Windows agent installation package. These components include drivers that prevent tampering and keep the agent running.	See "What gets installed for DLP Agents installed on Windows endpoints" on page 91.

Installing the DLP Agent for Windows manually

Table 8-6 provides instructions for installing the 15.0 DLP Agent for Windows manually.

Note: These steps assume that you have generated the agent installation package. See "Generating agent installation packages" on page 79.

Table 8-6 Instructions for installing the DLP Agent for Windows manually

Step	Action	Description
1	Run the DLP Agent installer batch file.	You run the `install_agent.bat` located in the agent installation package ZIP file. **Note:** To troubleshoot the manual installation, you can remove the `/q` element from the `install_agent.bat` file. Removing the `/q` element launches the installation wizard which can provide error information. You can also review the installation log file (`installAgent.log` located at `C:\`) for additional troubleshooting information.
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. See "Confirming that the Windows agent is running" on page 91.

Installing DLP Agents for Windows silently

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

These steps assume that you have generated the agent installation package. See "Generating agent installation packages" on page 79.

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

To perform a silent installation

1 Specify the `InstallAgent.bat` file in your systems management software package.

2 Specify the `InstallAgent.bat` installation properties. The installation properties in the `InstallAgent.bat` file are based on entries and selections made during the agent installation packaging process. Symantec recommends that you do not update the installation properties.

When you install the Symantec DLP Agent, your systems management software issues a command to the specified endpoints. The following table summarizes important commands:

`msiexec`	The Windows command for executing MSI packages.
`/i`	Specifies the name of the package.
`/q`	Specifies a silent install. You can remove this command to install an agent using the wizard. You might install using this method if you want to test the installation package when preparing to run a silent installation.
`ARPSYSTEMCOMPONENT`	Optional properties to `msiexec`.
`ENDPOINTSERVER`	The Endpoint Server to which agents will connect. This value is defined during the agent installation packaging process.
`SERVICENAME`	The agent service name. The default value is `EDPA`.
`INSTALLDIR`	The location where the agent is installed on the endpoint: `C:\Program Files\Manufacturer\Symantec DLP Agent\`. This value is defined during the agent installation packaging process.
`UNINSTALLPASSWORDKEY`	The password the administrator uses when uninstalling agents. This value is defined during the agent installation packaging process.
`WATCHDOGNAME`	The watchdog service name: `WDP`.

`TOOLS_KEY`	The password associated with the agent tools. This value is defined during the agent installation packaging process.
`ENDPOINT_CERTIFICATE`	The endpoint self-signed certificate file name: `endpoint_cert.pem`. This file is created during the agent installation packaging process.
`ENDPOINT_PRIVATEKEY`	The endpoint private key file name: `endpoint_priv.pem`. This file is created during the agent installation packaging process.
`ENDPOINT_TRUSTSTORE`	The endpoint trust store file to trust the server certificate (server public key): `endpoint_truststore.pem`. This file is created during the agent installation packaging process.
`ENDPOINT_PRIVATEKEY_PASSWORD`	The password associated with the agent certificates. The password is located in the `endpoint_priv.pem` file, which is created during the agent installation packaging process.

The following is an example of what the completed 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="<generated endpoint private key password>"
VERIFY_SERVER_HOSTNAME="No" STARTSERVICE="Yes" ENABLEWATCHDOG="YES"
LOGDETAILS="Yes" /log C:\installAgent.log
```

3 Specify any optional properties for the `msiexec` utility.

Confirming that the Windows agent is running

After you install the agents, the Symantec DLP Agent service automatically starts on each endpoint. Log on to the Enforce Server and go to **System > Agents > Overview**. Verify that the newly installed or upgraded agents are registered (that the services appear in the list).

The watchdog service is deployed with the DLP Agent on Windows endpoints. The watchdog is a service that ensures that the DLP Agent is running and active. This relationship is reciprocal. If the DLP Agent does not receive regular requests from the watchdog service, it automatically restarts the watchdog service. This reciprocal relationship ensures that the DLP Agent is always running and active.

Users cannot stop the watchdog service on their workstations. Preventing users from stopping the watchdog service allows the DLP Agent to remain active on the endpoint.

What gets installed for DLP Agents installed on Windows endpoints

The DLP Agent installation places a number of components on endpoints. Do not disable or modify any of these components or the DLP Agent may not function correctly.

Table 8-7 Installed components

Component	Description
Driver (`vfsmfd.sys`)	Detects any activity in the endpoint file system (including activity on Citrix XenApp and XenDesktop) and relays the information to the DLP Agent service. This driver is installed at `<Windows_dir>\System32\drivers`. For example, `c:\windows\System32\drivers`. All other agent files are installed into the agent installation directory.
Driver (`vnwcd.sys`)	Intercepts network traffic (HTTP, FTP, and IM protocols) on the endpoint. After the Symantec Data Loss Prevention Agent analyzes the content, the `vnwcd.sys` driver allows or blocks the data transfer over the network. This driver is installed at `<Windows_dir>\System32\drivers`. For example, `c:\windows\System32\drivers`. All other agent files are installed into the agent installation directory.

Table 8-7 Installed components *(continued)*

Component	Description
Driver (`vrtam.sys`)	Monitors the process creation and destruction, and send notifications to the DLP Agent. The driver monitors the applications that are configured as part of Application Monitoring; for example, CD/DVD applications. This driver is installed at `<Windows_dir>\System32\drivers`. For example, `c:\windows\System32\drivers`. All other agent files are installed into the agent installation directory.
Symantec DLP Agent service	Receives all information from the driver and relays it to the Endpoint Server. During installation, the DLP Agent is listed under the task manager as `edpa.exe`. Users are prevented from stopping or deleting this service on their workstation.
Watchdog service	Automatically checks to see if the DLP Agent is running. If the DLP Agent has been stopped, the watchdog service restarts the DLP Agent. If the watchdog service has been stopped, the DLP Agent service restarts the watchdog service. Users are prevented from stopping or deleting this service.

The DLP Agent service creates the following files:

- Two log files (`edpa.log` and `edpa_ext0.log`), created in the installation directory.
- Each DLP Agent maintains an encrypted database at the endpoint called the DLP Agent store. The DLP Agent store saves two-tier request metadata, incident information, and the original file that triggered the incident, if needed. Depending on the detection methods used, the DLP Agent either analyzes the content locally or sends it to the Endpoint Server for analysis.
- A database named `rrc.ead` is installed to maintain and contain non-matching entries for rules results caching (RRC).

Process to install the DLP Agent on Mac

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

Before you install DLP Agents on Mac endpoints, confirm that you have completed prerequisite steps. See "DLP Agent installation overview" on page 77.

Table 8-8 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 install an agent, or to insert in your SMS to install agents to many Mac endpoints. You can also add endpoint tools to the package and add a custom package identifier.	See "Packaging Mac agent installation files" on page 93.
2	Install the agent. You can install the agent manually when you install a single agent to test the configuration. Install the agents using your SMS. You install agents using this method to install many agents at one time.	See "Installing the DLP Agent for Mac manually" on page 95. See "Installing DLP Agents on Mac endpoints silently" on page 96.
3	Confirm that the Mac agent service is running.	See "Confirming that the Mac agent is running" on page 97.
4	(Optional) Review the installed Mac agent components. These components include the drivers that prevent tampering and keep the agent running.	See "What gets installed for DLP Agents on Mac endpoints" on page 97.

Packaging Mac agent installation files

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

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 78.

To package the Mac agent installation 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 82.

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

`$ cd /tmp/MacInstaller`	Defines the path where the Mac agent installation 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 95.

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 "Installing DLP Agents on Mac endpoints silently" on page 96.

About optional installation and maintenance tools

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

The tools can be found in the following files:

- Installation tools are found in the `SymantecDLPMacAgentInstaller_15.0.zip` file
- Maintenance tools are found in the `SymantecDLPMacAgentTools_15.0.zip` file
  See "About Endpoint tools" on page 110.

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 installation files" on page 93.

Table 8-9 lists the available tools.

Table 8-9 Mac agent installation and maintenance tools

Tool type	Description
Installation	■ Agent.ver adds agent package versioning information. ■ Start_agent restarts the Mac agents that have been shut down on the **Agent List** screen. See "Starting DLP Agents that run on Mac endpoints" on page 108. ■ Uninstall_agent uninstalls the DLP Agent from Mac endpoints. See "Removing a DLP Agent from a Mac endpoint" on page 138.
Maintenance	■ Vontu_sqlite3 lets you inspect the agent database. ■ Logdump creates agent log files.

Installing the DLP Agent for Mac manually

Table 8-10 provides steps for installing 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 "Installing DLP Agents on Mac endpoints silently" on page 96.

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 78.

Table 8-10 Instructions for installing 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`.
2	Install 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_0.pkg -target /` Replace `/tmp/MacInstaller` with the path where you unzipped the agent installation package.
3	Verify the Mac agent installation.	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 installation.	If you experience installation 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_0.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 installed for DLP Agents on Mac endpoints" on page 97.

Installing DLP Agents on Mac endpoints silently

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

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

See "Generating agent installation packages" on page 79.

See "Packaging Mac agent installation files" on page 93.

To perform an unattended installation

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 install the DLP Agent.
5. Start the silent installation process.

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

Confirming that the Mac agent is running

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

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

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

See "What gets installed for DLP Agents on Mac endpoints" on page 97.

What gets installed 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 8-11 Mac agent components

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

About Endpoint tools

Symantec Data Loss Prevention provides a number of tools to help you work with Symantec DLP Agents. See the *Acquiring Symantec Data Loss Prevention Software* document for information on obtaining the files that contain these tools.

Move these tools to a secure directory. The Endpoint tools work with the keystore file that is found in the Agent Install directory. The tools and the keystore file must be in the same folder to function properly.

Note: Before you copy Endpoint tools to the Agent Install directory on Mac endpoints, change the permissions for each tool to be executable.

Each tool requires a password to operate. You enter the Endpoint tools password during the agent packaging process. You can manage the Endpoint tools password using the **Agent Password Management** screen.

See "Generating agent installation packages" on page 79.

See "About agent password management" on page 109.

Table 8-12 lists some of the tasks that you can complete using endpoint tools:

Table 8-12 Endpoint tools task list

Task	Tool name and location	Additional information
Shut down the agent and the watchdog services	service_shutdown Available for Windows agents in the `Symantec_DLP_15.0_Agent_Win-IN.zip` file. Available for Mac agents in the `Symantec_DLP_15.0_Agent_Mac-IN.zip` file.	See "Shutting down the agent and the watchdog services on Windows endpoints" on page 101. See "Shutting down the agent service on Mac endpoints" on page 101.
Inspect database files that are accessed by the agent	vontu_sqlite3 Available for Windows agents in the `Symantec_DLP_15.0_Agent_Win-IN.zip` file. Available for Mac agents in `Symantec_DLP_15.0_Agent_Mac-IN.zip` file.	See "Inspecting the database files accessed by the agent" on page 102.
View extended log files	logdump Available for Windows agents in the `.Symantec_DLP_15.0_Agent_Win-IN.zip` file. Available for Mac agents in the `Symantec_DLP_15.0_Agent_Mac-IN.zip` file.	See "Viewing extended log files" on page 103.
Generate device information	`DeviceID.exe` for Windows removable devices. Available for Windows agents in the `Symantec_DLP_15.0_Agent_Win-IN.zip` file. `DeviceID` for Mac removable devices. Available for Mac agents in the `Symantec_DLP_15.0_Agent_Mac-IN.zip` file.	See "About the Device ID utilities" on page 104.

Table 8-12 Endpoint tools task list *(continued)*

Task	Tool name and location	Additional information
Generate third-party application information	GetAppInfo Available for Windows agents in the `Symantec_DLP_15.0_Agent_Win-IN.zip` file.	
Start DLP Agents that are installed on Mac endpoints	`start_agent` Available for Mac agents in the `AgentInstaller_Mac64.zip` file. This file is created after you complete the agent installation package process. See "Generating agent installation packages" on page 79. **Note:** You must unzip this file to a Mac endpoint. You cannot use the tool if it is unzipped to a Windows endpoint.	See "Starting DLP Agents that run on Mac endpoints" on page 108.

Using Endpoint tools with Windows 7/8/8.1

If you use Endpoint tools on a computer that runs Windows 7/8/8.1, run the command prompt in the Elevated Command Prompt mode. This procedure is required because of the nature of the Windows operating system. You cannot run the Endpoint tools without using the Elevated Command Prompt mode.

To initiate the Elevated Command Prompt mode on Windows 7

1. Click the **Start** menu.
2. In the **Search programs and files** field, enter **command prompt**.

   The **Command Prompt** program appears in the results list.
3. Hold the Shift key and right-click the **Command Prompt** entry in the results list. Select either **Run as Administrator** or **Run as different user**.
4. If you selected **Run as different user**, enter the credentials for a user that has administrator privileges.

To initiate the Elevated Command Prompt mode on Windows 8/8.1

1. Display the Command Prompt.
   - In Desktop mode, right-click on the Windows icon and select **Command Prompt (Admin)**, then click the **Start** menu.

- In Metro mode, enter **cmd** in the **Search programs and files** field.

2 Hold the Shift key and right-click **Command Prompt** in the results list.

3 Select **Run as Administrator**.

Shutting down the agent and the watchdog services on Windows endpoints

The Service_Shutdown.exe tool enables you to shut down the DLP Agent and watchdog services on Windows endpoints. As a tamper-proofing measure, it is not possible for a user to individually stop either the DLP Agent or watchdog service. This tool enables users with administrator rights to stop both Symantec Data Loss Prevention services at the same time.

To run the Service_Shutdown.exe tool

- From the installation directory, run the following command:

  ```
  service_shutdown [-p=password]
  ```

  where the installation directory is the directory where you installed Symantec Data Loss Prevention and `[-p=password]` is the password you previously specified. If you do not enter a password, you are prompted to input a password. The default password is *VontuStop*.

  You must run the Service_Shutdown.exe tool from the same directory as the DLP Agent keystore file.

See "About Endpoint tools" on page 110.

Shutting down the agent service on Mac endpoints

The Service_Shutdown tool enables you to shut down the DLP Agent service on Mac endpoints. As a tamper-proofing measure, users cannot stop the DLP Agent service on Mac endpoints. However, an administrator with root access can use the Service_Shutdown tool to stop the Symantec Data Loss Prevention service.

To stop the agent on Mac endpoints:

1 Set the Service_Shutdown tool permissions to be executable.

2 Copy the Service_Shutdown tool to the DLP Agent installation folder on the Mac endpoint.

3 Run the following command as a root user using the Terminal application:

```
#sudo ./service_shutdown

-p=<tools_password>
```

See "About Endpoint tools" on page 110.

Inspecting the database files accessed by the agent

The `vontu_sqlite3` tool enables you to inspect the database files that the DLP Agent uses. It provides an SQL interface to query database files and update database files. Without this tool, you cannot view the contents of a database file because it is encrypted. Use this tool when you want to investigate or make changes to the Symantec Data Loss Prevention files.

Note: You must have administrator rights to use the tool on Windows endpoints. You must have root or sudo access to make changes to the agent database on Mac endpoints.

To run the vontu_sqlite3.exe tool on Windows endpoints

1. Run the following script from the Symantec Data Loss Prevention Agent installation directory:

   ```
   vontu_sqlite3 -db=database_file [-p=password]
   ```

   where *database_file* is your database file and `password` is your specified tools password.

   The Symantec Data Loss Prevention database files for Windows agents are located in the DLP Agent installation directory and end in the `*.ead` extension. After you run the command, you are prompted for your password.

2. Enter the default password `VontuStop` unless you have already created a unique password.

   You are provided with a shell to enter SQL statements to view or update the database.

   Refer to http://www.sqlite.org/sqlite.html for complete documentation about what commands are available in this shell.

To run the vontu_sqlite3 tool on Mac endpoints

1. Set the vontu_sqlite3 tool permissions to be executable.
2. Run the following script from the Symantec Data Loss Prevention Agent installation directory:

   ```
   sudo ./vontu_sqlite3 -db=database_file [-p=password]
   ```

   where *database_file* is your database file and `password` is your specified tools password.

   You run this command using the Terminal application. The `vontu_sqlite3` tool is located at `/Library/Manufacturer/Endpoint Agent/`.

3. Enter the default password `VontuStop` unless you have already created a unique password.

   You are provided with a shell to enter SQL statements to view or update the database.

   Refer to http://www.sqlite.org/sqlite.html for complete documentation about what commands are available in this shell.

See “About Endpoint tools” on page 110.

Viewing extended log files

The logdump.exe tool enables users with administrator privileges to view the extended log files for Symantec Data Loss Prevention Agents. Extended log files are hidden for security reasons. Generally, you only need to view log files with Symantec Data Loss Prevention support personnel. Without this tool, you cannot view any Symantec Data Loss Prevention Agent log files.

Note: You must have administrator rights to use the tool on Windows endpoints. You must have root or sudo access to make changes to the agent database on Mac endpoints.

To run the log dump tool on Windows endpoints

1 Run the following script from the Symantec Data Loss Prevention Agent installation directory:

```
logdump -log=log_file [-p=password]
```

where *log_file* is the log file you want to view and *password* is the specified tools password. All Symantec Data Loss Prevention extended log files are present in the Symantec Data Loss Prevention Agent installation directory. The files have names of the form edpa_ext*file_number*.log. After you run this command, you can see the de-obfuscated log.

Note: When using Windows PowerShell to run `logdump.exe`, quotes are required around the log file. For example, run:

```
logdump "-log=log_file" [-p=password]
```

All Symantec Data Loss Prevention extended log files are present in the Symantec Data Loss Prevention Agent installation directory. The files have names of the form edpa_ext*file_number*.log. After you run this command, you can see the de-obfuscated log.

2 (Optional) Print the contents of another log from this view.

To run the log dump tool on Mac endpoints

1 Set the logdump tool permissions to be executable.

2 Run the following scripts from the Symantec Data Loss Prevention Agent installation directory:

```
sudo ./logdump -log=log_file [-p=password]
```

where *log_file* is the log file you want to view and *password* is the specified tools password.

All Symantec Data Loss Prevention extended log files are present in the Symantec Data Loss Prevention Agent installation directory. The files have names of the form edpa_ext*file_number*.log. After you run this command, you can see the de-obfuscated log.

3 (Optional) Print the contents of another log from this view.

To print the contents of another log

1 From the command window, run:

```
logdump -log=log_file -p=password > deobfuscated_log_file_name
```

2 Enter the password again to print the log.

See "About Endpoint tools" on page 110.

About the Device ID utilities

Symantec Data Loss Prevention provides the `DeviceID.exe` for Windows removable devices and the `DeviceID` for Mac removable devices to assist you with configuring endpoint devices for detection.

The DeviceID utilities scan the computer for all connected devices and reports the Device Instance ID string on Windows endpoints and regex information on Mac endpoints.

You typically use the DeviceID utilities to allow the copying of sensitive information to company-provided external devices like USB drives and SD cards.

See "Using the Windows Device ID utility" on page 105.

See "Using the Mac Device ID utility" on page 107.

Table 8-13 Windows Device ID utility example output

Result	Description
Volume	The volume or mount point that the `DeviceID.exe` tool found. For example: `Volume: E:\`
Dev ID	The Device Instance ID for each device. For example: `USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\5F73HF00Y9DBOG0DXJ`
Regex	The regular expression to detect that device instance. For example: `USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\5F73HF00Y9DBOG0DXJ`

Table 8-14 Mac Device ID utility example output

Result	Description
Vendor	The vendor that the DeviceID tool found. For example: `SanDisk&.*`
Model	The model that the DeviceID tool found. For example: `SanDisk&Cruzer Blade&.*`
Serial	The serial number that the DeviceID tool found. For example: `SanDisk&Cruzer Blade&DER45TG5444`

Using the Windows Device ID utility

Use the Device ID utility to extract Device Instance ID strings and to determine what devices the system can recognize for detection. You must have administrator rights to use this tool.

See "About the Device ID utilities" on page 104.

To use the Device ID utility

1 Obtain the `DeviceID.exe` utility.

This utility is available with the Endpoint Server utilities package.

See "About Endpoint tools" on page 110.

2 Copy the `DeviceID.exe` utility to a computer where you want to determine Device IDs.

3 Install the devices you want to examine onto the computer where you copied the `DeviceID.exe` utility.

For example, plug in one or more USB devices, connect a hard drive, and so forth.

4 Run the `DeviceID.exe` utility from the command line.

For example, if you copied the `DeviceID.exe` utility to the C:\temp directory, issue the follow command:

```
C:\TEMP>DeviceID
```

To output the results to a file, issue the following command:

```
C:\TEMP>DeviceID > deviceids.txt
```

The file appears in the C:\temp directory and contains the output from the DeviceID process.

5 View the results of the DeviceID process.

The command prompt displays the results for each volume or mount point.

See Table 8-13 on page 105.

6 Use the DeviceID utility to evaluate the proposed regex string against a device that is currently connected.

See Table 8-15 on page 106.

7 Use the regular expression patterns to configure endpoint devices for detection.

Table 8-15 Device ID regex evaluation

Command parameters	Example
DeviceID.exe [-m] [Volume] [Regex]	`DeviceID.exe -m E:\ "USBSTOR\\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\\.*"` **Note:** The regex string needs to be inside quotation marks.
Returns	**Match!** or **Not match!**

Using the Mac Device ID utility

Use the Mac Device ID utility to generate regex information. You use this feature to allow the copying of sensitive information to company-provided external devices like USB drives and SD cards.

See "About the Device ID utilities" on page 104.

To use the Device ID utility

1. Obtain the `DeviceID` utility.

   This utility is available with the Mac agent tools package.

   See "About Endpoint tools" on page 110.

2. Copy the `DeviceID` utility to a computer where you want to determine Device IDs.
3. Install the devices you want to examine onto the computer where you copied the `DeviceID` utility.

   For example, plug in one or more USB devices, connect a hard drive, and so on.

4. Run the `DeviceID` utility from the Terminal application.

   For example, if you copied the `DeviceID` utility to the `Downloads` directory, issue the follow command:

   `$HOME/Downloads/DeviceID` where `$HOME` is your home directory.

   The output results display information for each volume or mount point in the Terminal application dialog.

5. Review the DeviceID process results.
6. Use the regex information to configure endpoint devices for detection.

Table 8-16

Command parameter	Example
`./DeviceID > deviceids.txt`	The tool outputs the following information to the `deviceids.txt` file based on information gathered from the attached thumb drive: ■ Volume: */Volumes/FAT_USB/* ■ Type (BUS): *USB* ■ Device ID Regex by Vendor: *JetFlash&.** ■ Device ID Regex by Model: *JetFlash&Mass Storage Device&.** ■ Device ID Regex by Serial No: *JetFlash&Mass Storage Device&79HCSMJ0RYOHT2FE*

Starting DLP Agents that run on Mac endpoints

You can use the start_agent tool to start DLP Agents that run on Mac endpoints. You use the tool if the agents have been shut down using the shutdown task on the **Agent List** screen.

This tool is available in the `AgentInstaller_Mac64.zip` file. This file is created after you complete the agent installation package process. See "Generating agent installation packages" on page 79.

Note: You must unzip this file to a Mac endpoint. You cannot use the tool if it is unzipped to a Windows endpoint.

To start agents using the start_agent tool:

1. Set the start_agentn tool permissions to be executable.
2. From the Symantec Data Loss Prevention Agent installation directory, run the following command:

   ```
   sudo ./start_agent
   ```

   where the installation directory is the directory where you installed Symantec Data Loss Prevention.
3. Go to the **Agent List** screen and confirm that the agent is running.

See "About Endpoint tools" on page 110.

About uninstallation passwords

The uninstallation password prevents unauthorized users from removing the DLP Agent from an endpoint. If an unauthorized user tries to remove the agent without the password, the agent cannot be removed.

You create or assign the password during agent installation or after installation using the **Agent Password Management** screen in the Enforce Server administration console. When you want to remove an agent from an endpoint, the uninstallation password parameter pop-up window requests the uninstallation password. If you remove agents from a large number of endpoints using an agent management system, the password must be included in the uninstallation command line.

See "Generating agent installation packages" on page 79.

See "About agent password management" on page 109.

See "Using uninstallation passwords" on page 109.

Using uninstallation passwords

When you want to uninstall a DLP Agent that is password protected, you must enter the correct password before the uninstallation continues. If you uninstall your agents manually, a pop-up window appears on the endpoint that requests the password. You must enter the password in this window. If you are using system management software, include the password parameter in the command string.

Note: By default, the limit for how many times an administrator can enter the wrong password is 3. If the limit is exceeded, the uninstallation process quits and the process must be restarted. You can adjust the default value using the UninstallPassword.RETRY_LIMIT advanced agent setting.

If you want to uninstall a group of agents, specify the uninstallation password in the agent uninstallation command line.

To enter the uninstallation password using a command line

- Enter the following parameter in the uninstallation command line;

  `UNINSTALLPASSWORD="<password>"`

  where `<password>` is the password that you specified in the password generator.

An agent command line looks like the following example:

`msiexec /uninstall <product code> /q UNINSTALLPASSWORD="<password>"`

See "Generating agent installation packages" on page 79.

See "About agent password management" on page 109.

See "About uninstallation passwords" on page 108.

Upgrading agents and uninstallation passwords

When you upgrade agents, the uninstallation password that was previously applied is removed. To apply an uninstallation password, you enter one during the agent packaging process. You can apply a new password using the **Agent Password Management** screen.

See "About agent password management" on page 109.

See "About uninstallation passwords" on page 108.

About agent password management

You use the **Agent Password Management** screen (**System > Agents > Agent Passwords**) to add or change the DLP Agent uninstallation password and Endpoint tools password. The

uninstallation password prevents unauthorized users from removing the Symantec DLP Agent. The Endpoint tools password grants access to various agent management tools.

Note: Only administrators with the Server Administrator role can use the **Agent Password Management** screen.

When you create or change a password, the password is applied to the agents when they connect to the Endpoint Server. Likewise, uninstall passwords or Endpoint tools passwords that are created during the agent packaging process are retained until the agents connect to the Endpoint Server.

You can disable the uninstall password for select agents on the **Agent List** screen.

You can use the **Agent Password Management** screen to complete the following agent password-related tasks:

- Create a new uninstall or Endpoint tools password if one was not created during the agent packaging process.
- Change an existing uninstall password or Endpoint tools password.
- Retain a password created during the agent packaging process. You can choose whether or not to publish an uninstall password or Endpoint tools password to newly added agents by de-selecting the checkbox for each password.

See “Generating agent installation packages” on page 79.

See “About Endpoint tools” on page 110.

Chapter 9

Post-installation tasks

This chapter includes the following topics:

About post-installation tasks

You must perform certain required tasks after a product installation or upgrade is complete. There are also some optional post-installation tasks that you might want to perform.

See "About post-installation security configuration" on page 112.

See "About system events and syslog servers" on page 126.

See "Enforce Servers and unused NICs" on page 127.

See "Performing initial setup tasks on the Enforce Server" on page 127.

Note: The Enforce Server administration console requires the use of cookies. Ensure that you have enabled cookies in the web browser you use to access the Enforce Server administration console.

About post-installation security configuration

Symantec Data Loss Prevention secures communications between all Symantec Data Loss Prevention servers. This task is accomplished by encrypting the transmitted data and requiring servers to authenticate with each other.

Symantec Data Loss Prevention also secures data communications and authenticates between the Endpoint Server and Symantec DLP Agent.

Although the default installation is secure, Symantec recommends that you change your system's default security settings to use unique certificates or keys.

See "About browser certificates" on page 113.

See "Symantec Data Loss Prevention directory and file exclusion from antivirus scans" on page 116.

See "Corporate firewall configuration" on page 118.

About server security and SSL/TLS certificates

Symantec Data Loss Prevention uses Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt all data that is transmitted between servers. It also uses the SSL/TLS protocol for mutual authentication between servers. Servers implement authentication by the mandatory use of client and server-side certificates.

The Enforce Server administration console web application enables users to view and manage incidents and policies and to configure Symantec Data Loss Prevention. You access this interface with a web browser. The Enforce Server and browser communicate through a secure SSL/TLS connection. To ensure confidentiality, all communication between the Enforce Server and the browser is encrypted using a symmetric key. During connection initiation, the Enforce Server and the browser negotiate the encryption algorithm. The negotiation includes the algorithm, key size, and encoding, as well as the encryption key itself.

A "certificate" is a keystore file used with a keystore password. The terms "certificate" and "keystore file" are often used interchangeably. By default, all the connections between the Symantec Data Loss Prevention servers, and the Enforce Server and the browser, use a self-signed certificate. This certificate is securely embedded inside the Symantec Data Loss Prevention software. By default, every Symantec Data Loss Prevention server at every customer installation uses this same certificate.

Although the existing default security meets stringent standards, Symantec provides the `keytool` and `sslkeytool` utilities to enhance your encryption security:

- The `keytool` utility generates a new certificate to encrypt communication between your web browser and the Enforce Server. This certificate is unique to your installation.
  See "About browser certificates" on page 113.
  See "Generating a unique browser certificate" on page 114.

- The `sslkeytool` utility generates new SSL server certificates to secure communications between your Enforce Server and your detection servers. These certificates are unique to your installation. The new certificates replace the single default certificate that comes with all Symantec Data Loss Prevention installations. You store one certificate on the Enforce Server, and one certificate on each detection server in your installation.

  Note: Symantec recommends that you create dedicated certificates for communication with your Symantec Data Loss Prevention servers. When you configure the Enforce Server to use a generated certificate, all detection servers in your installation must also use generated certificates. You cannot use the built-in certificate with some detection servers and the built-in certificate with other servers.

  Note: If you install a Network Prevent detection server in a hosted environment, you must generate unique certificates for your Symantec Data Loss Prevention servers. You cannot use the built-in certificate to communicate with a hosted Network Prevent server.

  See "About the sslkeytool utility and server certificates" on page 49.
  See "Using sslkeytool to generate new Enforce and detection server certificates" on page 52.

See "About post-installation tasks" on page 111.

You may also need to secure communications between Symantec Data Loss Prevention servers and other servers such as those used by Active Directory or a Mail Transfer Agent (MTA). See the *Symantec Data Loss Prevention Administration Guide* for details.

About browser certificates

A web browser using a secure connection (HTTPS) requires an SSL certificate. The SSL certificate can be self-signed or signed by a certificate authority. With a certificate, the user authenticates to other users and services, or to data integrity and authentication services, using digital signatures. It also enables users to cache the public keys (in the form of certificates) of their communicating peers. Because a certificate signed by a certificate authority is automatically trusted by browsers, the browser does not issue a warning when you connect to the Enforce Server administration console. With a self-signed certificate, the browser issues a warning and asks if you want to connect.

The default certificate installed with Symantec Data Loss Prevention is a standard, self-signed certificate. This certificate is embedded securely inside the Symantec Data Loss Prevention software. By default, all Symantec Data Loss Prevention installations at all customer sites use this same certificate. Symantec recommends that you replace the default certificate with a new, unique certificate for your organization's installation. The new certificate can be either self-signed or signed by a certificate authority.

See "Generating a unique browser certificate" on page 114.

See "About server security and SSL/TLS certificates" on page 112.

Generating a unique browser certificate

By default, connections between the Enforce Server and the browser use a single, self-signed certificate. This certificate is embedded securely inside the Symantec Data Loss Prevention software.

The `keytool` utility manages keys and certificates. This utility enables users to administer their own public and private key pairs and associated certificates for use in self-authentication.

To generate a unique Enforce Server self-signed certificate for your installation

1. Collect the following information:
   - Common Name: The fully qualified DNS name of the Enforce Server. This must be the actual name of the server accessible by all the clients.
     For example, `https://Server_name`.
   - Organization Name: The name of your company or organization.
     For example, Acme, Inc.
   - Organizational unit : The name of your division, department, unit, etc. (Optional)
     For example, Engineering
   - City: The city, town, or area where you are located.
     For example, San Francisco
   - State: The name of your state, province, or region.
     For example, California or CA
   - Country: Your two-letter country code.
     For example, US
   - Expiration: The certificate expiration time in number of days.
     For example: 90
2. Stop all the Vontu services on the Enforce Server.

   See "About Symantec Data Loss Prevention services" on page 129.
3. On the Enforce Server, go to the `\SymantecDLP\jre\bin` directory.

   The `keytool` software is located in this directory.
4. Use `keytool` to create the self-signed certificate (keystore file). This keystore file can also be used to obtain a certificate from a certificate authority.

   From within the `\bin` directory, run the following command with the information collected earlier:

```
keytool -genkey -alias tomcat -keyalg RSA -keysize 1024
  -keystore .keystore -validity NNN -storepass protect
  -dname "cN=common_name, O=organization_name,
  Ou=organization_unit, L=city, S=state, C=XX"
```

Where:

- The `-alias` parameter specifies the name of this certificate key. This name is used to identify this certificate when you run other keytool commands. The value for the `-alias` parameter must be `tomcat`.
- The `-keystore` parameter specifies the name and location of the keystore file which must be `.keystore` located in this directory. This is specified by using `-keystore .keystore`
- The `-keyalg` parameter specifies the algorithm to be used to generate the key pair. In this case, the algorithm to specify is **RSA**.
- The `-keysize` parameter specifies the size of each key to be generated. For example, **1024**.
- The `-validity` parameter specifies the number of days the certificate is good for. For example, `-validity 365` specifies that the certificate is good for 365 days (or one year). The number of days you choose to specify for the `-validity` parameter is up to you. If a certificate is used for longer than the number of days specified by `-validity`, an "Expired" message appears by the browser when it accesses the Enforce Server administration console. The best practice is to replace an expired certificate with a new one.
- The `-storepass` parameter specifies the password used to protect the integrity of the keystore. The value for the `-storepass` parameter must be `protect`.
- The `dname` parameter specifies the X.500 Distinguished Name to be associated with this alias. It is used as the issuer and subject fields in a self-signed certificate. The parameters that follow are the value of the `dname` parameter.
- The `-CN` parameter specifies your name. For example, `CN=linda wu`
- The `O` parameter specifies your organization's name. For example, `O=Acme Inc.`
- The `Ou` parameter specifies your organization's unit or division name. For example, `Ou=Engineering Department`
- The `L` parameter specifies your city. For example, `L=San Francisco`
- The `S` parameter specifies your state or province. For example, `S=California`
- The `C` parameter specifies the two-letter countrycode of your country. For example, `C=US`

- If you are asked for a keypass password, hit Return to make the keypass password the same as the storepass password.

An updated `.keystore` file is generated.

5 (Optional) Rename or move the existing `.keystore` file from the `\Protect\tomcat\conf` directory.

6 Copy the updated `.keystore` file into the `c:\SymantecDLP\Protect\tomcat\conf` directory.

7 Restart the Vontu services on the Enforce Server.

See "About Symantec Data Loss Prevention services" on page 129.

As an alternative to using a self-signed certificate, you can use a certificate issued by an internal or external certificate authority (CA). Consult your certificate authority for instructions on how to obtain a CA-signed certificate. Certificate authorities provide a root certificate and a signed certificate. When using certificates signed by a CA, they need to be imported into the Enforce Server using the following commands:

```
keytool -import -alias root -keystore .keystore -trustcacerts -file root_certificate
keytool -import -alias tomcat -keystore .keystore -trustcacerts -file signed_certificate
```

See "About server security and SSL/TLS certificates" on page 112.

About Symantec Data Loss Prevention and antivirus software

Symantec recommends installing antivirus software on your Symantec Data Loss Prevention servers. However, antivirus software may interpret Symantec Data Loss Prevention activity as virus-like behavior. Therefore, certain files and directories must be excluded from antivirus scans. These files and directories include the Symantec Data Loss Prevention and Oracle directories on your servers. If you do not have antivirus software installed on your Symantec Data Loss Prevention servers (not recommended), you can skip these antivirus-related post-installation tasks.

See "Symantec Data Loss Prevention directory and file exclusion from antivirus scans" on page 116.

See "Oracle directory and file exclusion from antivirus scans" on page 117.

See "About post-installation tasks" on page 111.

Symantec Data Loss Prevention directory and file exclusion from antivirus scans

When the Symantec Data Loss Prevention application accesses files and directories, it can appear to antivirus software as if it were a virus. Therefore, you must exclude certain directories from antivirus scans on Symantec Data Loss Prevention servers.

Using your antivirus software, remove the following Enforce Server directories from antivirus scanning:

- `\SymantecDLP\Protect\incidents`
- `\SymantecDLP\Protect\index`
- `\SymantecDLP\Protect\logs` (with subdirectories)
- `\SymantecDLP\Protect\temp` (with subdirectories)
- `\SymantecDLP\Protect\tomcat\temp`
- `\SymantecDLP\Protect\tomcat\work`

Using your antivirus software, remove the following detection server directories from antivirus scanning:

- `\drop`
- `\drop_pcap`
- `\icap_spool`
- `\packet_spool`
- `\SymantecDLP\Protect\incidents`
- `\SymantecDLP\Protect\index`
- `\SymantecDLP\Protect\logs` (with subdirectories)
- `\SymantecDLP\Protect\temp` (with subdirectories)

Consult your antivirus software documentation for information on how to exclude directories and files from antivirus scans.

See "About Symantec Data Loss Prevention and antivirus software" on page 116.

See "Oracle directory and file exclusion from antivirus scans" on page 117.

See "About post-installation tasks" on page 111.

Oracle directory and file exclusion from antivirus scans

When the Symantec Data Loss Prevention application accesses files and directories, it can appear to antivirus software as if it were a virus. Therefore, you must exclude certain directories from antivirus scans on Symantec Data Loss Prevention servers.

Using your antivirus software, exclude the following Oracle directories from antivirus scanning:

- `C:\app\Administrator\oradata\protect`
- `C:\app\Administrator\product\11.2.0.4\dbhome_1`

Most of the Oracle files to be excluded are located in these directories, but additional files are located in other directories. Use the Oracle Enterprise Manager (OEM) to check for additional files and exclude their directories from antivirus scanning. Use OEM to view the location of the following database files:

- Data files, which have the file extension `*.DBF`
- Control files, which have the file extension `*.CTL`
- The `REDO.LOG` file

Exclude all the directories with these files from antivirus scanning.

See "About Symantec Data Loss Prevention and antivirus software" on page 116.

See "Symantec Data Loss Prevention directory and file exclusion from antivirus scans" on page 116.

See "About post-installation tasks" on page 111.

Corporate firewall configuration

If the Enforce Server is installed inside your corporate LAN behind a firewall and your detection servers are installed in the DMZ your corporate firewall settings need to:

- Allow connections from the Enforce Server on the corporate network to the detection servers in the DMZ. Configure your firewall to accept connections on the port you entered when installing the detection servers. By default, the Enforce Server and the detection servers communicate over port 8100. You can configure the servers to use any port higher than 1024. Use the same port number for all your detection servers.
- Allow Windows Remote Desktop Client connections (TCP port 3389). This feature can be useful for setup purposes.

Symantec Data Loss Prevention servers communicate with the Enforce Server over a single port number. Port 8100 is the default, but you can configure Symantec Data Loss Prevention to use any port higher than 1024. Review your firewall settings and close any ports that are not required for communication between the Enforce Server and the detection servers.

Windows security lockdown guidelines

You should complete a set of hardening procedures after you install or upgrade a Symantec Data Loss Prevention server. Adapt these guidelines to suit your organization's standards for secure communications and hardening procedures.

The following Windows services must be running:

- Alerter
- COM+ Event System

- DCOM Server Process Launcher
- Defwatch for Symantec (may not always be present)
- DNS Client
- Event log
- Interix Subsystem Startup (for UNIX Services for Windows for RAs)
- IPSEC Services
- Logical Disk Manager
- Network connections
- OracleOraDb11g_home1TNSListener
  The service name is different if you use a non-default Oracle home directory.
- OracleServicePROTECT (on the Enforce Server only)
- Plug and play
- Protected Storage
- Remote procedure call (RPC)
- Removable Storage
- Security Accounts Manager
- Server (required only for Enforce if EDMs are used)
- Symantec AntiVirus
- System Event Notification
- Task Scheduler
- TCP/IP NetBIOS Helper Service
- Terminal Services
- User Name Mapping (for UNIX Services for Windows for RAs)
- `VontuIncidentPersister` (for Enforce Server only)
- `VontuManager` (for Enforce Server only)
- `VontuMonitor` (for detection servers only)
- `VontuNotifier` (for Enforce Server only)
- `VontuUpdate`
- Windows Management (Instrumentation)
- Windows Management (Instrumentation Driver Extensions Workstation)

- Windows Time (required if no alternative Enforce/detection server system clock synchronization is implemented)
- Workstation (required for Alerter Service)

The following Windows services should be disabled:

- Dist. File System
- Dist. Link Tracking Client
- Dist. Link Tracking Server
- Dist. Transaction Coordinator
- Error Reporting Service
- Help & Support
- Messenger
- Print Spooler
- Remote Registry
- Wireless Config

Consult your Windows Server documentation for information on these services.

Windows Administrative security settings

The following tables provide recommended administrative settings available on a Microsoft Windows system for additional security hardening.

Consult your Windows Server documentation for information on these settings.

The following Local Policy settings are described in the following tables:

- Table 9-1 lists the **Account Lockout Policy** settings.
- Table 9-2 lists the **Password Policy** settings.
- Table 9-3 lists the local **Audit Policy** settings.
- Table 9-4 lists the **User Rights Assignment** settings.
- Table 9-5 lists the **Security Options** settings.

Table 9-1 Security settings > Account Policies > Account Lockout Policy

Policy	Recommended security settings
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts

Table 9-1 Security settings > Account Policies > Account Lockout Policy *(continued)*

Policy	Recommended security settings
Reset account lockout counter after	15 minutes

Table 9-2 Security settings > Account Policies > Password Policy

Password policy	Recommended security settings
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	2 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Table 9-3 Security settings > Local Policies > Audit Policy

Local audit	Recommended security settings
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Table 9-4 Security settings > Local Policies > User rights assignment

User rights assignment	Recommended security settings
Restore files and directories	Administrators, Backup Operators
Shut down the system	Administrators, Power Users, Backup Operators

Table 9-4 Security settings > Local Policies > User rights assignment *(continued)*

User rights assignment	Recommended security settings
Synchronize directory service data	
Take ownership of files or other objects	Administrators
Access this computer from the network	Everyone, Administrators, Users, Power Users, Backup Operators
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE, NETWORK SERVICE, Administrators
Allow log on locally	Administrators, Users, Power Users, Backup Operators
Allow log on through Services	Administrators, Remote Desktop Users
Back up files and directories	Administrators, Backup Operators
Bypass traverse checking	Everyone, Administrators, Users, Power Users, Backup Operators
Change the system time	Administrators, Power Users
Create a page file	Administrators
Create a token object	
Create global objects	Administrators, SERVICE
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delegation	

Table 9-4 Security settings > Local Policies > User rights assignment *(continued)*

User rights assignment	Recommended security settings
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE, NETWORK SERVICE
Impersonate a client after authentication	Administrators, SERVICE
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	LOCAL SERVICE
Log on as a service	NETWORK SERVICE
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators, Power Users
Profile system performance	Administrators
Remove computer from docking station	Administrators, Power Users
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Administrators, Backup Operators
Shut down the system	Administrators, Power Users, Backup Operators
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Table 9-5 Security settings > Local Policies > Security options

Security options	Recommended security settings
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Table 9-5 Security settings > Local Policies > Security options *(continued)*

Security options	Recommended security settings
Accounts: Rename administrator account	protectdemo
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Do not allow installation
Domain controller: Allow server operators to schedule tasks	Enabled
Domain controller: LDAP machine signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable server account password changes	Disabled

Table 9-5 Security settings > Local Policies > Security options *(continued)*

Security options	Recommended security settings
Domain member: Maximum server account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require domain controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	Force Logoff
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Table 9-5 Security settings > Local Policies > Security options *(continued)*

Security options	Recommended security settings
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of credentials or passwords for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, EPMAPPER, LOCATOR, TrkWks, TrkSvr
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\ CurrentVersion
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog

See "About post-installation tasks" on page 111.

About system events and syslog servers

Symantec Data Loss Prevention enables you to send severe system events to a syslog server. Configuring a syslog server in this manner can be helpful after installation to help identify problems with the initial deployment. To enable syslog logging, you must modify the `Manager.properties` file in the config directory.

See the *Symantec Data Loss Prevention System Maintenance Guide* for more information about using a syslog server.

Note: As an alternative to syslog logging, you can configure Symantec Data Loss Prevention to send email notifications of severe system events. See the online Help for details.

Enforce Servers and unused NICs

If the Enforce Server has multiple NICs, disable the unused NICs if possible. If the unused NIC cannot be disabled, make the following changes to the properties file. These changes enable the detection servers to talk to the Enforce Server.

On the Enforce Server `\SymantecDLP\Protect\config\model.properties` file:

```
model.notification.host=IP
model.notification.serverobject.host=IP
```

On the detection server `\SymantecDLP\Protect\config\model.properties` file:

```
model.notification.host=IP
\SymantecDLP\Protect\bin\NotificationTrafficMonitor.lax
lax.command.line.args=IP:37328
```

Where *IP* is the IP address that you want to bind on.

Performing initial setup tasks on the Enforce Server

Immediately after installing the Enforce Server, you should perform these initial tasks to set up Symantec Data Loss Prevention.

See the *Symantec Data Loss Prevention Administration Guide* and online Help for information on how to perform these tasks.

To initially set up Symantec Data Loss Prevention

1. If you have not already done so, back up the unique `CryptoMasterKey.properties` file for your installation and store the file in a safe place. This file is required for Symantec Data Loss Prevention to encrypt and decrypt the Enforce Server database.

   Warning: If the unique `CryptoMasterKey.properties` file becomes lost or corrupted, you must restore a copy of the file in order for Symantec Data Loss Prevention to function. The Enforce Server database cannot be decrypted without the corresponding `CryptoMasterKey.properties` file.

2. If you use password authentication, change the Administrator's password to a unique password known only to you.
3. Add an email address for the Administrator user account so you can be notified of system events.
4. Add user accounts for all users who are authorized to use the system, and provide them with their log on information.

5 If you are responsible for adding policies, add one or more policies.

If not, notify the policy administrator(s) that data profiles have been added and they can proceed with policy addition. Be sure that you have added user accounts with policy access for each policy administrator in your organization and provided them with their logon information.

6 Configure any detection servers that you registered with the Enforce Server.

7 If you installed Network Discover, set up Discover targets.

8 Determine your organization's incident management workflow and add incident attributes.

You can continue to add data profiles, policies, and reports, and modify your settings to suit your organization's needs.

Chapter 10

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 10-1 Symantec Data Loss Prevention services

Service Name	Description
Vontu Manager	Provides the centralized reporting and management services for Symantec Data Loss Prevention.
Vontu Detection Server Controller	Controls the detection servers.
Vontu Notifier	Provides the database notifications.
Vontu Incident Persister	Writes the incidents to the database.

Table 10-1 Symantec Data Loss Prevention services *(continued)*

Service Name	Description
Vontu Update	Installs the Symantec Data Loss Prevention system updates.

See "About starting and stopping services on Windows" on page 130.

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 130.
- See "Stopping an Enforce Server on Windows" on page 131.
- See "Starting a Detection Server on Windows" on page 131.
- See "Stopping a Detection Server on Windows" on page 131.
- See "Starting services on single-tier Windows installations" on page 132.
- See "Stopping services on single-tier Windows installations" on page 132.

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:
   - `VontuNotifier`
   - `VontuManager`
   - `VontuIncidentPersister`
   - `VontuMonitorController` (if applicable)
   - `VontuUpdate` (if necessary)

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

See "Stopping an Enforce Server on Windows" on page 131.

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:
   - `VontuMonitorController` (if applicable)
   - `VontuIncidentPersister`
   - `VontuManager`
   - `VontuNotifier`
   - `VontuUpdate` (if necessary)

See "Starting an Enforce Server on Windows" on page 130.

Starting a Detection Server on Windows

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

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Start the Symantec Data Loss Prevention services, which might include the following services:
   - `VontuMonitor`
   - `VontuUpdate`

See "Stopping a Detection Server on Windows" on page 131.

Stopping a Detection Server on Windows

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

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

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the **Services** menu, stop all running Symantec Data Loss Prevention services, which might include the following services:

- VontuUpdate
- VontuMonitor

See "Starting a Detection Server on Windows" on page 131.

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:
   - VontuNotifier
   - VontuManager
   - VontuIncidentPersister
   - VontuMonitorController (if applicable)
   - VontuMonitor
   - VontuUpdate (if necessary)

Note: Start the VontuNotifier service before starting other services.

See "Stopping services on single-tier Windows installations" on page 132.

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:
   - VontuMonitor

- `VontuMonitorController` (if applicable)
- `VontuIncidentPersister`
- `VontuManager`
- `VontuNotifier`
- `VontuUpdate` (if necessary)

See "Starting services on single-tier Windows installations" on page 132.

Chapter 11

Uninstalling Symantec Data Loss Prevention

This chapter includes the following topics:

Uninstalling a server or component from a Windows system

You can uninstall Symantec Data Loss Prevention from a Windows-based Enforce Server or detection server. You can uninstall Symantec Data Loss Prevention by:

- Using **Add or Remove Programs** control from the Windows **Control Panel**
- Double-clicking on the `c:\SymantecDLP\uninstall.exe` file
- Running `c:\SymantecDLP\uninstall.exe` from the command line
- Selecting **Start > All Programs > Symantec DLP > Symantec DLP Uninstaller**

Note: Uninstalling Symantec Data Loss Prevention also removes the incremental scan index that is used with Network Discover. If you want to preserve the incremental scan index, back it up before you uninstall Symantec Data Loss Prevention. See the *Symantec Data Loss Prevention System Maintenance Guide* for information about backing up the incremental scan index.

To uninstall a Windows server

1. Before running the uninstaller, ensure that you have backed up all keystore files in the `c:\SymantecDLP\Protect\keystore` directory
2. Run `c:\SymantecDLP\uninstall.exe`. Or 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.
3. Click **Next** to display the **Preserve Reinstallation Resources** panel.
4. Select **Preserve Reinstallation Resources** to indicate that the uninstaller should not remove the `CryptoMasterKey.properties` file or the keystore files.

   Note: Each Symantec Data Loss Prevention installation encrypts its database using a unique `CryptoMasterKey.properties` file, and uses unique keystore files for Endpoint certificate management. Exact copy of these file are required if you intend to reuse the existing Symantec Data Loss Prevention database and Endpoint Servers. Preserving your Enforce Schema during uninstallation creates an `EnforceReinstallationResources.zip` file containing both the `CryptoMasterKey.properties` and keystore files, which you can use during the reinstallation process. If the `EnforceReinstallationResources.zip` file becomes lost or corrupted and you do not have a backup, contact Symantec Technical Support to recover the file.
5. Click **Next** to uninstall Symantec Data Loss Prevention.
6. Click **Finish** to complete the uninstall process.

   If you chose to save the `EnforceReinstallationResources.zip`, it is preserved in the `c:\SymantecDLP` directory.

About Symantec DLP Agent removal

You may need to uninstall the Symantec DLP Agent from your endpoints. You can uninstall Symantec DLP Agents in the following ways:

Table 11-1 Removing the Symantec DLP Agent

Removing a DLP Agent from a Windows endpoint
Removing DLP Agents from Windows endpoints using system management software
Removing DLP Agents from Mac endpoints using system management software

Table 11-1 Removing the Symantec DLP Agent *(continued)*

Removing a DLP Agent from a Mac endpoint

Removing DLP Agents from Windows endpoints using system management software

Follow this procedure if you elected to hide the Symantec Data Loss Prevention service from the Add or Remove Programs list (ARP) during installation. Because the Symantec DLP Agent does not appear in the ARP, you cannot use the ARP list for the uninstallation process. You must use the MSI command to remove the Symantec DLP Agent. Only use the MSI command uninstallation if you have hidden the Symantec DLP Agent from the ARP during installation.

To remove the agent with the MSI command

1. Open the command prompt window.
2. Enter the string:

   ```
   msiexec /x AgentInstall_15_0.msi
   ```

   You can add several different options to this command prompt.
3. Click **OK**.

   The Symantec DLP Agent uninstalls.

To remove the agent manually if the agent does not appear in the ARP

1. Open the command prompt window.
2. Enter the following command where [*guid*] is the product code. You can locate the GUID from the Windows registry or in the `uninstall_agent.bat` file.

   You can add several other options to this command prompt:

   ```
   msiexec /x {guid}
   ```
3. Enter any optional commands to the end of the command:

   ```
   msiexec /x AgentInstall_15_0.msi
   ```

4 Click **OK**.

You can add options to the uninstall command such as `SilentMode` or `Logname`. `SilentMode` allows the Symantec DLP Agent to uninstall without displaying a user interface on the desktop. The installation takes place in the background of the workstation and is not visible to the user. `Logname` Lets you set any log file you want. However, this option is only available if you have the original installer present. If you do not have the original installer, you must use the product code.

The code for a silent install is:

```
/QN:silentmode
```

The code for `Logname` is:

```
/L*V _logname
```

`msi.exe` has several other options. For further options, see your MSI guide.

See "About Symantec DLP Agent removal" on page 135.

Removing a DLP Agent from a Windows endpoint

You can uninstall Symantec DLP Agents manually. Manual uninstallation is only possible if you configured the Symantec DLP Agent to appear in the endpoint **Add or Remove Programs** list during deployment.

Note: You uninstall Windows 7/8/8.1 agents in **Elevated Command Prompt** mode. See "Using the Elevated Command Prompt with Windows" on page 85.

See "Process to install the DLP Agent on Windows" on page 86.

To uninstall the agent manually

1 Go to **Start > Control Panel** and double-click **Add or Remove Programs**.

2 Select **Agent Install**.

3 Click **Remove**.

See "About Symantec DLP Agent removal" on page 135.

Removing DLP Agents from Mac endpoints using system management software

Use the following steps to remove DLP Agents from Mac endpoints using your system management software (SMS).

To remove the agent

1 Locate the uninstall_agent command and copy it to a temporary location on the endpoint.

This tool is located in the `Symantec_DLP_15.0_Agent_Mac-IN.zip` file.

2 Add the uninstall command to your SMS.

```
sudo / /tmp/uninstall_agent -prompt=n

/rm -f /tmp/uninstall_agent
```

Replace */tmp* with the location where the `uninstall_agent` command is located.

3 Identify agents to be uninstalled and run the uninstallation.

Removing a DLP Agent from a Mac endpoint

You can uninstall the Mac DLP Agent by running the uninstaller tool from the default agent installation location: `/Library/Manufacturer/Endpoint Agent`.

To uninstall the DLP Agent from Mac endpoints

1 Open the Terminal app.

2 Run this command:

```
$sudo ./uninstall_agent
```

Note: You can review uninstall logs on the Terminal application by running this command: `sudo ./uninstall_agent -prompt=no -log=console`. By default, logs are saved to the `uninstall_agent.log` file

---

Appendix A

Installing Symantec Data Loss Prevention with the FIPS encryption option

This appendix includes the following topics:

About FIPS encryption

The Federal Information Processing Standards 140-2 (FIPS) are federally defined standards on the use of cryptography. Using FIPS encryption is not generally recommended for most customers because it requires additional computational overhead.

Before you enable FIPS encryption, you must contact your Symantec representative.

You should install Symantec Data Loss Prevention with FIPS encryption enabled only if your organization must comply with FIPS regulations (typical organizations include US government agencies and departments). If you do not choose to use FIPS encryption, the installer defaults to standard encryption. After you have installed Symantec Data Loss Prevention, you cannot switch to a different encryption option except by reinstalling Symantec Data Loss Prevention. When a re-installation is required, old incidents are not preserved.

See “Installing Symantec Data Loss Prevention with FIPS encryption enabled” on page 140.

Note: You must install all Symantec Data Loss Prevention servers with the same encryption option; you cannot mix encryption options. If the Endpoint Prevent Server is installed with FIPS enabled, no additional configuration is required to enable FIPS encrypted communication with your DLP Agents.

If your organization uses Internet Explorer to access the Enforce Server, then you must ensure that Internet Explorer is configured to use FIPS.

See "Configuring Internet Explorer when using FIPS" on page 140.

Installing Symantec Data Loss Prevention with FIPS encryption enabled

To run Symantec Data Loss Prevention with FIPS encryption, Symantec Data Loss Prevention has to be installed with FIPS enabled.

See "About FIPS encryption" on page 139.

To install the Symantec Data Loss Prevention software with FIPS encryption enabled

- When installing each Symantec Data Loss Prevention server, execute the ProtectInstaller with the `-VJCEProviderType=FIPS` command-line argument:

  ```
  ProtectInstaller64_15.0.exe -VJCEProviderType=FIPS
  ```

  When this command is entered correctly, the first panel of the Installation Wizard notifies you that the system is being installed with FIPS encryption enabled.

  See "Installing an Enforce Server" on page 23.

  See "Installing a detection server" on page 40.

  See "Installing a single-tier server " on page 65.

If your organization uses Internet Explorer to access the Enforce Server administration console, you must ensure that Internet Explorer is configured to use FIPS.

See "Configuring Internet Explorer when using FIPS" on page 140.

Configuring Internet Explorer when using FIPS

If you have installed Federal Information Processing Standards (FIPS) support, you must enable TLS 1.0 protocol support in Internet Explorer to access Symantec Data Loss Prevention with that browser.

Note: Firefox is already FIPS compatible. You do not need to perform the steps in this section to access Symantec Data Loss Prevention with Firefox.

You must first enable TLS 1.0 protocol support in Internet Explorer, and then enable FIPS compliance in Windows. This procedure must be done on all Windows computers in your organization that access the Symantec Data Loss Prevention Enforce Server administration console.

To enable TLS 1.0 protocol support in Internet Explorer

1. Go to **Tools > Internet Options**.
2. Go to the **Advanced** tab.
3. Scroll down to the Security settings.
4. Make sure that the following check boxes are selected: Use SSL 2.0, Use SSL 3.0, and Use TLS 1.0.
5. Click **Apply**.
6. Click **OK**.

   Internet Explorer on all computers that access the Enforce Server must be configured to use the TLS 1.0 protocol.

All Windows computers that access the Enforce Server administration console with an Internet Explorer browser must be configured for FIPS compliance.

To enable FIPS compliance in Windows

1. Open the Windows Control Panel.
2. Double-click **Administrative Tools**.
3. Double-click **Local Security Policy**.
4. In the Local Security Settings, double-click **Local Policies**.
5. Double-click **Security Options**.
6. In the **Policy** pane on the right, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
7. Choose the **Enabled** radio button and then click **Apply**.

Index

T

U

V

W