Symantec™ Data Loss Prevention Installation Guide for Windows

Version 11.6

Symantec Data Loss Prevention Installation Guide for Windows

Documentation version: 11.6a

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Planning the Symantec Data Loss Prevention installation

This chapter includes the following topics:

About accessing the Symantec Data Loss Prevention Knowledgebase

In addition to your product documentation, the Symantec Data Loss Prevention Knowledgebase is a valuable resource for information. The Knowledgebase provides solutions to common problems, troubleshooting tips, and other useful information. In addition, important product announcements, updated release notes and product guides, and product bulletins are published at the Knowledgebase.

The Knowledgebase is available at https://kb-vontu.altiris.com.

You must create an account with a user name and password to access the Knowledgebase. All Data Loss Prevention users are strongly encouraged to create a Knowledgebase account.

To create an account

1. Navigate to the Knowledgebase login page at https://kb-vontu.altiris.com.
2. Click the **New User** link to request access.

It may take several days to process your request.

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 only for performing risk assessments or testing the software.

Single-tier	To implement the single-tier installation, you install the database, the Enforce Server, and a detection server all on the same computer. Use single-tier installation only for testing or risk assessment purposes. See "Performing a single-tier installation—high-level steps" on page 23. See "Registering a detection server" on page 61.

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 20.
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 17.

About 64-bit operating system support

Symantec Data Loss Prevention servers run in 64-bit mode on supported 64-bit operating systems. In multi-tier Symantec Data Loss Prevention deployments, the Enforce Server and detection servers can use any combination of 32-bit and 64-bit server software. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for a complete list of compatible 32-bit and 64-bit operating systems for Symantec Data Loss Prevention server computers.

To install a Symantec Data Loss Prevention server with 64-bit support, use the designated 64-bit installer for your platform. Using the correct installer copies the required 64-bit files and configures the server for 64-bit operating systems.

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. The options provided at installation time are:

- 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 SPC authentication or certificate authentication.
- SPC authentication and sign-on.
  You can optionally integrate the Enforce Server with a single Symantec Protection Center (SPC) instance. With SPC integration, a user first logs into the SPC console, and may then access the Enforce Server administration console from within the SPC interface. If you choose SPC authentication, the installation program also enables password 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 either password authentication or SPC authentication, no additional information is required during the Symantec Data Loss Prevention installation. However, to use the SPC authentication mechanism you must register an SPC instance with the Enforce Server after you install Symantec Data Loss Prevention.

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 SPC authentication or 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.

The Enforce Server and all other detection servers must reside in the corporate network and communicate over a LAN. Only Network Prevent for Email and Network Prevent for Web can be deployed to a hosted environment.

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.

Note: Mobile Prevent is not supported in a hosted environment.

See "Installing a detection server" on page 57.

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 47.

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 materials

Most hardware and software requirements are described in the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*. In addition, before you start to install Symantec Data Loss Prevention, make sure that the following materials are available.

- Your Symantec Data Loss Prevention software.
  As explained in the *Acquiring Symantec Data Loss Prevention Software* document, before installing Symantec Data Loss Prevention you must download and extract the Symantec Data Loss Prevention software ZIP files. These ZIP files must be extracted into a directory on a system that is accessible to you. The root directory into which the ZIP files are extracted is referred to as the `DLPDownloadHome` directory.
- Your Symantec Data Loss Prevention license file.
  As explained in the *Acquiring Symantec Data Loss Prevention Software* document, before installing Symantec Data Loss Prevention you must 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`.
- The Oracle database software is included in the Symantec Data Loss Prevention installation package. You must install Oracle software before installing the Enforce Server.
  See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for details.

Also, some or all of the following third-party components are required:

- Network Monitor servers require either a dedicated NIC or a high-speed packet capture adapter (either Endace or Napatech).

- Windows-based Network Monitor servers require WinPcap software. WinPcap software is recommended for all detection servers. The WinPcap software is located in the *DLPDownloadHome*\DLP\Symantec_DLP_11.6_Win\11.6_Win\Third_Party\ directory. 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 other than 4.1.1.
- 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.
- Mobile Prevent requires specially configured VPN and proxy servers. See the *Symantec Data Loss Prevention Administration Guide*.
- 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\Vontu` 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
Step 1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 25.
Step 2	Verify that your servers are ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.
Step 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* for information about installing Oracle.
Step 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.
Step 5	Install the Enforce Server.	See "Installing an Enforce Server" on page 29.
Step 6	Verify that the Enforce Server is correctly installed.	See "Verifying an Enforce Server installation" on page 39.

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

Step	Action	Description
Step 7	Import a solution pack.	See "Importing a solution pack" on page 42. See "About Symantec Data Loss Prevention solution packs" on page 41.
Step 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 47.

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

Step	Action	Description
Step 9	If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, you can optionally implement and configure the Symantec Management Platform to manage endpoints with the Symantec Management Console. Installing and using the Symantec Management Console with Symantec Data Loss Prevention is optional. However, the Symantec Management Console offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention.	See "About the Symantec Management Console" on page 89. See the *Symantec Data Loss Prevention Administration Guide* for information about other ways to manage endpoint computers for Endpoint Discover and Endpoint Prevent.
Step 10	Install a detection server.	See "Installing a detection server" on page 57.
Step 11	Register a detection server.	See "Registering a detection server" on page 61.
Step 12	Perform the post-installation tasks.	See "About post-installation tasks" on page 95.
Step 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 95. 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
Step 1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 25.
Step 2	Verify that your servers are ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.
Step 3	Install Oracle and create the Symantec Data Loss Prevention database.	See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.
Step 4	Install the Enforce Server.	See "Installing an Enforce Server" on page 29.
Step 5	Verify that the Enforce Server is correctly installed.	See "Verifying an Enforce Server installation" on page 39.
Step 6	Import a solution pack.	See "Importing a solution pack" on page 42. See "About Symantec Data Loss Prevention solution packs" on page 41.

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

Step	Action	Description
Step 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 47.
Step 8	If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, you can optionally implement and configure the Symantec Management Platform to manage endpoints with the Symantec Management Console. Installing and using the Symantec Management Console with Symantec Data Loss Prevention is optional. However, the Symantec Management Console offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention.	See "About the Symantec Management Console" on page 89. See the *Symantec Data Loss Prevention Administration Guide* for information about other ways to manage endpoint computers for Endpoint Discover and Endpoint Prevent.
Step 9	Install a detection server.	See "Installing a detection server" on page 57.

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

Step	Action	Description
Step 10	Register a detection server.	See "Registering a detection server" on page 61.
Step 11	Perform the post-installation tasks.	See "About post-installation security configuration" on page 95.
Step 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 95. 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. Single-tier installations are not recommended for production environments.

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	Description
Step 1	Perform the preinstallation steps.	See "Symantec Data Loss Prevention preinstallation steps" on page 25.
Step 2	Verify that the server is ready for installation.	See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.

Table 1-3 Performing a single-tier installation—high-level steps *(continued)*

Step	Action	Description
Step 3	Install Oracle and create the Symantec Data Loss Prevention database.	See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.
Step 4	Install the Enforce Server and a detection server on the same computer.	See "Installing a single-tier server" on page 63.
Step 5	Verify that the Enforce Server is correctly installed.	See "Verifying a single-tier installation" on page 72.
Step 6	Import a solution pack.	See "About Symantec Data Loss Prevention solution packs" on page 41. See "Importing a solution pack" on page 42.
Step 7	If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, you can optionally implement and configure the Symantec Management Platform to manage endpoints with the Symantec Management Console. Installing and using the Symantec Management Console with Symantec Data Loss Prevention is optional. However, the Symantec Management Console offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention.	See "About the Symantec Management Console" on page 89. See the *Symantec Data Loss Prevention Administration Guide* for information about other ways to manage endpoint computers for Endpoint Discover and Endpoint Prevent.
Step 8	Register the detection server.	See "Registering a detection server" on page 61.

Table 1-3 Performing a single-tier installation—high-level steps *(continued)*

Step	Action	Description
Step 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 95. 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 16.
- You have gathered the required materials.
  See "Symantec Data Loss Prevention required materials" on page 16.

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. Turn off the Microsoft Auto Update feature. Contact your Symantec representative before installing any new patches. Symantec verifies new Microsoft patches and sends you a communication when it is safe to apply new patches to Symantec Data Loss Prevention servers.
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 27.

8 Copy the following files from *DLPDownloadHome* to an easily accessible directory on the Enforce Server:

- The Symantec Data Loss Prevention installer: `ProtectInstaller_11.6.exe` for 32-bit platforms or `ProtectInstaller64_11.6.exe` for 64-bit platforms.
  These files can be found in the *DLPDownloadHome*`\DLP\Symantec_DLP_11_Win\11.6_Win\New_Installs\x86` and *DLPDownloadHome*`\DLP\Symantec_DLP_11_Win\11.6_Win\New_Installs\x64` directories.
- Your Symantec Data Loss Prevention license file.
  License files have names in the format *name*`.slf`.
- The appropriate solution pack file. Solution pack files have names ending in `*.vsp`.
  Solution pack files can be found in the *DLPDownloadHome*`\DLP\Symantec_DLP_11_Win\11.6_Win\Solution_Packs` directory.
  See "About Symantec Data Loss Prevention solution packs" on page 41.
- Symantec DLP Agent installer: `AgentInstall.msi` for 32-bit platforms or `AgentInstall64.msi` (for Windows 7 64-bit platforms).
  This file is only available if you licensed Endpoint Prevent.
- (Optional) Lookup SDK installer: `LookupSdkInstaller_11.6.exe`.
  Copy this file if you want to look up custom attributes from a corporate directory.
  This file can be found in the *DLPDownloadHome*`\DLP\Symantec_DLP_11_Win\11.6_Win\New_Installs` directory.

Note: These installation instructions assume that you copied these files into the `c:\temp` directory on the Enforce Server.

---

9 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.

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 datacenter.
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 116.
   - 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 materials" on page 16.

See "Symantec Data Loss Prevention preinstallation steps" on page 25.

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.

For a Network Prevent for Web Server installation, follow your proxy server integration guide to configure the proxy server.

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 25.
- Verify that the system is ready for installation.
  See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.
- 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:

`ProtectInstaller_11.6.exe` for 32-bit platforms or
`ProtectInstaller64_11.6.exe` for 64-bit platforms.

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 127.

Note: The following instructions assume that the `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.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 `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.exe` file (`c:\temp`).
4. Double-click `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.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 used for testing, training, and risk assessment; single-tier systems are not recommended for production environments.

Since 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, 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 default user name is "protect."

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.

---

13 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.

14 In the **Symantec Management Console** panel, optionally enter the host name or IP address of the Symantec Management Console server to use for managing Symantec Data Loss Prevention Endpoint Agents. If you are not using the Symantec Management Console to manage agents, leave the field blank. Click **Next**.

See "About the Symantec Management Console" on page 89.

If you have not purchased a license for Endpoint Prevent or Endpoint Discover, click **Next** to skip this step.

Note that you can add this host name or IP address later on the Enforce Server by navigating to **Administration > Settings > System Settings**. Then configure the Symantec Management Console setting.

15 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:

- 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.

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

17 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**.

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.

---

18 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.

19 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.

20 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
Symantec Protection Console	Select this option if you want to integrate the Enforce Server with a single Symantec Protection Center (SPC) instance. With SPC integration, a user first logs into the SPC console, and may then access the Enforce Server administration console from within the SPC interface. To fully integrate SPC with the Enforce Server, register an SPC instance and configure SPC users after the installation is complete. See the *Symantec Data Loss Prevention Administration Guide* for more information.
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, import the certificate authority (CA) certificates that are required to validate users' client certificates. You 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.
None	Select **None** if you want users to log onto the Enforce Server administration console using passwords that were 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 or SPC-integrated authentication after you complete the installation, using instructions in the *Symantec Data Loss Prevention Administration Guide*.

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 **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.

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 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 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 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 appears.

After a successful installation, a completion notice appears.

Select the **Start Services** check box to start the Symantec Data Loss Prevention services. The services can be also started or stopped through the operating system.

25 Click **Finish**.

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

27 Verify that the Enforce Server is properly installed.

See "Verifying an Enforce Server installation" on page 39.

28 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 41.

29 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 Vontu Update services, which run *username*_update (by default, "protect_update").

Symantec Data Loss Prevention includes the following services:

- Vontu Manager

- Vontu Incident Persister
- Vontu Notifier
- Vontu Update
- Vontu Monitor Controller

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.

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** 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_v11.6.vsp`).

Solution pack files are available in the following directory:

`DLPDownloadHome``\DLP\Symantec_DLP_11_Win\11.6_Win\Solution_Packs\`.

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

Table 3-1 Symantec Data Loss Prevention solution packs

Name	File name
Data Classification for Enterprise Vault Solution Pack	Data_Classification_Enterprise_Vault_v11.6.vsp
Energy & Utilities Solution Pack	Energy_v11.6.vsp
EU and UK Solution Pack	EU_UK_v11.6.vsp
Federal Solution Pack	Federal_v11.6.vsp
Financial Services	Financial_v11.6.vsp
Health Care Solution Pack	Health_Care_v11.6.vsp

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

Name	File name
High Tech Solution Pack	High_Tech_v11.6.vsp
Insurance Solution Pack	Insurance_v11.6.vsp
Manufacturing Solution Pack	Manufacturing_v11.6.vsp
Media & Entertainment Solution Pack	Media_Entertainment_v11.6.vsp
Pharmaceutical Solution Pack	Pharmaceutical_v11.6.vsp
Retail Solution Pack	Retail_v11.6.vsp
Telecom Solution Pack	Telecom_v11.6.vsp
General Solution Pack	Vontu_Classic_v11.6.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\Symantec_DLP_11_Win\11.6_Win\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 42.

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 10.x solution pack on a version 11.6 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 41.

   Note: You must use a version 11.6 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\Symantec_DLP_11_Win\11.6_Win\Solution_Packs\ to an easily accessible local directory.
4. In Windows Services, stop all Symantec Data Loss Prevention services except for the Notifier service. The Notifier service must remain running.

   Stop the following services:

   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor (if a single-tier installation)
   - Vontu Monitor Controller

   See "About Enforce Server services" on page 119.

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_v11.6.vsp` solution pack in the `\SymantecDLP` directory of the Enforce Server, you would enter:

```
SolutionPackInstaller.exe import c:\SymantecDLP\Financial_v11.6.vsp
```

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

8 Restart the Symantec Data Loss Prevention services you stopped.

Make sure the Vontu Notifier service is also running. If the Notifier service is not running, start Notifier first, and then start the other Symantec Data Loss Prevention services:

- Vontu Notifier
- Vontu Manager
- Vontu Monitor (if a single-tier installation)
- Vontu Incident Persister
- Vontu Update
- Vontu Monitor Controller

See "About Enforce Server services" on page 119.

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 53.
- On a single-tier installation register a detection server.
See "Registering a detection server" on page 61.

Chapter 4

Configuring certificates for secure communication

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.

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.

See "About sslkeytool command line options" on page 46.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 47.

See "Using sslkeytool to add new detection server certificates" on page 49.

See "About server security and SSL/TLS certificates" on page 96.

About sslkeytool command line options

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

The following command forms and options are available for `sslkeytool`:

- `-genkey [-dir=`*`directory`* `-alias=`*`aliasFile`*`]`

  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). Use this command form the first time you generate unique certificates for your Symantec Data Loss Prevention installation.

- `-list=`*`file`*

  Lists the content of the specified keystore file.

- `-alias=aliasFile -enforce=enforceKeystoreFile [-dir=directory]`
  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 specify the `-dir` argument, you must also place the Enforce Server keystore file in the specified directory. Use this command form to add new detection server certificates to an existing Symantec Data Loss Prevention installation.

For example, the command `sslkeytool -genkey` 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.

See "About the sslkeytool utility and server certificates" on page 45.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 47.

See "Using sslkeytool to add new detection server certificates" on page 49.

See "About server security and SSL/TLS certificates" on page 96.

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.

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 `c:\SymantecDLP\Protect\bin` directory where the `sslkeytool` utility is stored.

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
classification01
```

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 this example:

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`

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
- classification01.*timestamp*.sslKeyStore

5 Copy the certificate file whose name begins with `enforce` to the `c:\SymantecDLP\Protect\keystore` directory on the Enforce Server.

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 `c:\SymantecDLP\Protect\keystore` directory of each detection server in your system.

   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 Vontu Monitor Controller service on the Enforce Server and the Vontu Monitor 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 49.

See "About sslkeytool command line options" on page 46.

See "About the sslkeytool utility and server certificates" on page 45.

See "About server security and SSL/TLS certificates" on page 96.

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

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 `c:\SymantecDLP\Protect\bin` directory where the `sslkeytool` utility is stored.
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:

   ```
   copy ..\keystore\enforce.Fri_Jul_23_11_24_20_PDT_2010.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:

   ```
   endpoint02
   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:

   ```
   sslkeytool -alias=.\aliases.txt
     -enforce=enforce.Fri_Jul_23_11_24_20_PDT_2010.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 keystore that you specify.
7. Copy each new certificate file to the `c:\SymantecDLP\Protect\keystore` directory on the appropriate detection server computer.
8. Delete or secure any additional copies of the certificate files to prevent unauthorized access to the generated keys.
9. Restart the Vontu Monitor 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 Vontu Monitor Controller service on the Enforce Server computer.
2. Start each detection server or restart the Vontu Monitor 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 5

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 5-1. The Enforce Server manages all of these detection servers.

Table 5-1 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 5-1 Detection servers *(continued)*

Server Name	Description
Network Discover	Network Discover identifies unsecured confidential data that is exposed on open file shares and Web servers. 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 Server.
Network Prevent for E-mail	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 15.
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 15. **Note:** If your Symantec Data Loss Prevention license includes both Mobile Prevent and Network Prevent for Web, you install a single detection server called Network and Mobile Prevent for Web.

Table 5-1 Detection servers *(continued)*

Server Name	Description
Mobile Prevent for Web	Mobile Prevent for Web connects mobile devices to your corporate network through Wi-Fi access or through cellular 3G connectivity. Network traffic for webmail, third-party applications such as Yahoo and Facebook, and corporate email applications, including Microsoft Exchange ActiveSync, is sent through the HTTP/S protocol. Corporate email is sent through Microsoft ActiveSync as HTTP/S protocol information. Microsoft ActiveSync receives the information from the corporate proxy server after it has gone through detection and then sends the message to the corporate Exchange Server. Messages sent through common applications such as Facebook or Dropbox are either blocked or the sensitive information is redacted from the message, depending on your policies. **Note:** If your Symantec Data Loss Prevention license includes both Mobile Prevent and Network Prevent for Web, you install a single detection server called Network and Mobile Prevent for Web. **Note:** You cannot deploy Mobile Prevent in a hosted service environment.
Endpoint Prevent	Endpoint Prevent monitors the use of sensitive data on endpoint systems and detects endpoint policy violations.
Classification	A Classification Server analyzes email messages that are sent from a Symantec Enterprise Vault filter, and provides a classification result that Enterprise Vault can use to perform tagging, archival, and deletion as necessary. The Discovery Accelerator and Compliance Accelerator products can also use classification tags to filter messages during searches or audits. **Note:** The Classification Server is used only with the Symantec Data Classification for Enterprise Vault solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Data Classification for Enterprise Vault filter and Classification Server to communicate with one another. See the *Enterprise Vault Data Classification Services Integration Guide* for more information.

See "Detection servers and remote indexers" on page 56.

See "Detection server installation preparations" on page 56.

See "Installing a detection server" on page 57.

See "Verifying a detection server installation" on page 60.

See "Registering a detection server" on page 61.

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 57.

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 25.
- Verify that the system is ready for detection server installation.
  See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.
- Before you begin, make sure that you have access and permission to run the Symantec Data Loss Prevention installer software:
  `ProtectInstaller_11.6.exe` for 32-bit installations or `ProtectInstaller64_11.6.exe` for 64-bit installations.
- Before you begin, make sure that you have `WinPcap_4.1.1.exe`. This file is located in the *`DLPDownloadHome`*`\DLP\Symantec_DLP_11.6_Win\11.6_Win\Third_Party\` directory.

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 other than 4.1.1.
- 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.

See "Installing a detection server" on page 57.

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 53.

Note: Symantec recommends that you disable any antivirus, pop-up blocker, and registry-protection software before you begin the detection server installation process.

Note: The following instructions assume that the `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.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 56.
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 4.1.1 on the server computer. Follow these steps:

- Copy `WinPcap_4.1.1.exe` to a local drive. This file is located in the *`DLPDownloadHome`*`\DLP\Symantec_DLP_11.6_Win\11.6_Win\Third_Party\` directory.
- Double-click on `WinPcap_4.1.1.exe` and follow the on-screen installation instructions.
- Enter `yes`, then click **OK**.
- Double-click on the `pcapstart.reg` file in the `\11.6_Win\Third_Party\` directory to add WinPcap to the Windows registry.

4 Copy the Symantec Data Loss Prevention installer (`ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.exe`) from the Enforce Server to a local directory on the detection server.

`ProtectInstaller_11.6.exe` and `ProtectInstaller64_11.6.exe` are 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 `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.exe` file.

6 Double-click `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.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 15.

See "Using sslkeytool to generate new Enforce and detection server certificates" on page 47.

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, 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.

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.

15 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.

16 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.

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

18 Verify the detection server installation.

See "Verifying a detection server installation" on page 60.

19 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 61.

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 57.

To verify a detection server installation

1 If you selected the option **Start Services**, then confirm that the Vontu Monitor and Vontu Update 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 57.

See "Verifying a detection server installation" on page 60.

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 Server select **Network 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.
   - For Network Prevent for Email Server select **Network Prevent for E-mail.**
   - For Network Prevent for Web Server select **Network Prevent for Web.**
     If your Symantec Data Loss Prevention license includes both and Network Prevent for Web, you register a single detection server called **Network and Mobile Prevent for Web**.
   - For Mobile Prevent, select **Mobile Prevent for Web**.
     If your Symantec Data Loss Prevention license includes both Mobile Prevent for Web and Network Prevent for Web you register a single detection server called **Network and Mobile Prevent for Web**.
   - For Endpoint Server select **Endpoint.**
   - For Classification Server select **Classification.**

   See "About detection servers" on page 53.

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.)
- 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 Enforce Server services" on page 119.

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 6

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 25.
- Verify that the system is ready for installation.
  See "Verifying that servers are ready for Symantec Data Loss Prevention installation" on page 27.
- 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:
  `ProtectInstaller_11.6.exe` for 32-bit platforms or
  `ProtectInstaller64_11.6.exe` for 64-bit platforms.

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 `ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.exe` file, license file, and solution pack file have been copied into the `c:\temp` directory on the Enforce Server.

Single-tier installations are for testing, training, and risk assessment purposes. Single-tier installations are not recommended for production environments.

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 4.1.1 on the system before installing the detection server by performing the following steps in this order:
   - Copy `WinPcap_4.1.1.exe` to a local drive. This file is located in *`DLPDownloadHome`*`\DLP\Symantec_DLP_11.6_Win\11.6_Win\Third_Party\`
   - Double-click on `WinPcap_4.1.1.exe` and follow the on-screen installation instructions.
   - Reset the registry settings by running `pcapstart.reg`, which can be found in: *`DLPDownloadHome`*`\DLP\Symantec_DLP_11.6_Win\11.6_Win\Third_Party\WinPcap_4.1.1_Upgrade\`
   - Enter `yes`, then click **OK**.
3. Copy the Symantec Data Loss Prevention installer (`ProtectInstaller_11.6.exe` or `ProtectInstaller64_11.6.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_11.6.exe` file.
5. Double-click `ProtectInstaller_11.6.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 **Symantec Management Console** panel, optionally enter the host name or IP address of the Symantec Management Console server to use for managing Symantec Data Loss Prevention Endpoint Agents. If you are not using the Symantec Management Console to manage agents, leave the field blank. Click **Next**.

If you have not purchased a license for Endpoint Prevent or Endpoint Discover, click **Next** to skip this step.

See "About the Symantec Management Console" on page 89.

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

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

Click **Next**.

17 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.

18 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.

19 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.

20 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
Symantec Protection Console	Select this option if you want to integrate the Enforce Server with a single Symantec Protection Center (SPC) instance. With SPC integration, a user first logs into the SPC console, and may then access the Enforce Server administration console from within the SPC interface. To fully integrate SPC with the Enforce Server, you will need to register an SPC instance and configure SPC users after the installation is complete. See the *Symantec Data Loss Prevention Administration Guide* for more information.
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.
None	Select **None** 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 or SPC-integrated authentication after you complete the installation, using instructions in the *Symantec Data Loss Prevention Administration Guide*.

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 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 **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.

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 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 8 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 The installation process begins. After the 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 appears.

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

25 When the completion notice appears, select the **Start Services** check box and click **Finish** to start the Symantec Data Loss Prevention services.

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

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.

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

See "Verifying a single-tier installation" on page 72.

27 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 41.

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

See "Registering a detection server" on page 61.

29 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 Vontu Update services, which run *username*_update.

Symantec Data Loss Prevention includes the following services:

- Vontu Manager
- Vontu Incident Persister
- Vontu Notifier
- Vontu Update
- Vontu Monitor
- Vontu Monitor Controller

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 `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.

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 41.

After importing a solution pack, register a detection server.

See "Registering a detection server" on page 61.

Chapter 7

Installing Endpoint Prevent Agents

This chapter includes the following topics:

About Symantec DLP Agent Installation

You can install the agent software using either automated methods or you can install the agent software manually.

Before you begin, make sure that you have installed and configured an Endpoint Server. If you are using the Symantec Management Console (SMC) to install agents, the SMC must also be installed before you can begin agent installation.

What gets installed for Symantec DLP Agents

When the DLP Agent is installed onto an endpoint computer, a number of components are also installed. Do not disable or modify any of these components or the DLP Agent may not function correctly.

Table 7-1 Installed components

Component	Description
Driver (`vfsmfd.sys`)	Detects any activity in the endpoint file system 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 (`tdifd116.sys`)	Intercepts network traffic (HTTP, FTP, and IM protocols) on the endpoint computer. After the Symantec Data Loss Prevention Agent analyzes the content, the tdifd105.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.
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 the Endpoint Application Control; 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.

Table 7-1 Installed components *(continued)*

Component	Description
Driver (`SFsCtrx116.sys`)	Monitors activity on Citrix XenApp and XenDesktop. 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. This relationship is reciprocal. Users are prevented from stopping or deleting this service on their workstation.

The DLP Agent service creates the following files:

- Two log files (`edpa.log` and `edpa_ext.log`), created in the installation directory.
- Each DLP Agent maintains an encrypted database at the endpoint. The database stores 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).

About preinstallation steps for Symantec DLP Agents

Before you install the Symantec DLP Agent, identify all security applications that run on your endpoint computers. Then 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.

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.

Using the Elevated Command Prompt with Windows Vista and Windows 7

If you install agents on an endpoint computer that runs Windows Vista or Windows 7, you must run the command prompt in **Elevated Command Prompt** mode. This step is required because of the nature of the Windows Vista operating system. You cannot install the agent using the install_agent.bat script without first using the Elevated Command Prompt mode.

To initiate the Elevated Command Prompt mode on Windows Vista

1. Right-click the command prompt icon in the **Windows Start** menu.
2. Select **Run as Administrator**.

   The command prompt starts in Elevated Command Prompt mode. You can now install the Symantec DLP Agents on the endpoint computer.

If you install on Windows 7, the procedure for using the Elevated Command Prompt mode follows.

To initiate the Elevated Command Prompt mode on Windows 7

1. Click the **Start** menu.
2. In the **Search programs and files** field, type **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.
5. The command prompt starts in Elevated Command Prompt mode. Install the Symantec DLP Agents on the endpoint computer using this command prompt.

About the watchdog service

The watchdog service is deployed with the DLP Agent. 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 their workstation.

About Endpoint Server redundancy

You can configure the Symantec DLP Agent to connect to multiple Endpoint Servers. 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 Symantec 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 Symantec DLP Agent tries to reconnect to the original Endpoint Server for 60 minutes before it connects to another Endpoint Server.

When a Symantec 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 Symantec DLP Agent may connect.

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

You must specify the list of Endpoint Servers when you install the Symantec 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 Symantec 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.

About the AgentInstall.msi package

Symantec DLP Agents are installed, configured, or upgraded on endpoint computers using the AgentInstall.msi package (or AgentInstall64.msi package for Windows 7 64-bit platforms). The Symantec Management Console or Systems Management Server (SMS) executes the package in Silent Mode using the Windows `msiexec` installer. You can also run the package installer interactively on an endpoint computer by executing the AgentInstall.msi package itself.

The AgentInstall.msi package accepts various configuration properties regardless of which method you choose to install the Symantec DLP Agents. Table 7-2 describes the required properties and optional properties for AgentInstall.msi and AgentInstall64.msi.

Table 7-2 AgentInstall.msi and AgentInstall64.msi Properties

Property Name	Description	Required or Optional	Default Value
ENDPOINTSERVER	Specifies the host name or IP address of one or more Endpoint Servers that are separated by semicolons. An optional port number can follow each host name or IP address. If no port number is specified, the default port number is used. The default number is 8000. For example: `ENDPOINTSERVER="epserver.company.com; 10.67.20.36:8002"`	Required	None
ENABLEFIPS	Enables FIPS-compliant encryption. Set this property to "Yes" to enable FIPS encryption if needed.	Optional	Yes
KEY	The authentication key that the Symantec DLP Agent and Endpoint Server use to establish a secure connection. Agents include a default authentication key, but you can create your own key using the `endpointkeytool` utility. To use your own key, specify it with the `KEY` parameter during deployment and installation. If you decide to specify the key after installing Symantec DLP Agents, you must reinstall the Symantec DLP Agents to specify the key. See "About endpointkeytool utility" on page 102.	Optional	None (A common default key is used.)
SERVICENAME	Specifies the Symantec DLP Agent service name that appears in the service list of the endpoint computer. The Symantec DLP Agent appears as edpa.exe on the computer's task list.	Optional	EDPA

Table 7-2 AgentInstall.msi and AgentInstall64.msi Properties *(continued)*

Property Name	Description	Required or Optional	Default Value
STARTSERVICE	Determines whether the Symantec DLP Agent and watchdog service are started on the endpoint computer after installation. Set this property to No to disable starting the services after installation.	Optional	Yes
WATCHDOGNAME	Specifies the watchdog service name that appears in the service list on the endpoint computer. The watchdog appears as wdp.exe in the Task Manager.	Optional	WDP

The `msiexec` installer also has several public properties that are commonly used when you install the AgentInstall.msi package. These properties include:

- ARPSYSTEMCOMPONENT
  This property can prevent the Symantec DLP Agent from appearing in the endpoint computer's Add or Remove Programs (ARP) list. If you set this property to `1`, the Symantec DLP Agent does not appear in the list. By default, the property is set to `0`, which allows the Symantec DLP Agents to appear in the ARP list.
- INSTALLDIR
  This property specifies the installation directory. The default installation directory is *`install_dir`*`\Manufacturer\Endpoint Agent`. For example, `c:\Program Files\Manufacturer\Endpoint Agent`.

About uninstallation passwords

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

When you create or assign the password during agent installation, it cannot be changed unless the agent is removed and then reinstalled. When you want to remove an agent from an endpoint computer, the uninstallation password parameter pop-up window requests the uninstallation password. If you remove agents from a large number of endpoint computers using an agent management system, the password must be included in the uninstallation command line.

By default, there is a limit to how many times an administrator can enter the wrong password. If the limit is exceeded, the uninstallation process quits and the process must be restarted.

You generate a secure uninstallation password by using the UninstallPwdKeyGenerator.exe tool.

You can generate more than one password if you want to assign different passwords to different groups of endpoint computers.

See "Creating passwords with the password generation tool" on page 82.

See "Adding uninstallation passwords to agents" on page 83.

See "Upgrading agents and uninstallation passwords" on page 84.

See "Using uninstallation passwords" on page 83.

Creating passwords with the password generation tool

Use the uninstallation password generator tool to create a unique password key.

The name of the uninstallation password generator tool is UninstallPwdKeyGenerator.exe.

The uninstallation password prevents unauthorized users from removing the Symantec DLP Agent. The UninstallPwdKeyGenerator.exe tool works with the `PGPSdk.dll` file to create unique passwords. The tool and the file must be located in the same Administrator's tools directory to function. The UninstallPwdKeyGenerator.exe tool and the `PGPSdk.dll` file should be located in the Administrator tool directory by default.

Note: The UninstallPwdKeyGenerator.exe tool only works in Microsoft Windows environments. You cannot use this tool with any other operating system.

To create an uninstallation password

1. From a command window, navigate to the Symantec Data Loss Prevention keystore directory.
2. Enter the following command:

   `-xp=<uninstall password>`

   where *<uninstall password>* is the password that you want to use. Choose a unique password key.

A password key is generated. Enter this key in the command line when you install the agent.

See "Adding uninstallation passwords to agents" on page 83.

Adding uninstallation passwords to agents

Uninstallation passwords prevent unauthorized users from removing the Symantec DLP Agent from an endpoint computer.

Passwords can only be added to Symantec DLP Agents during agent installation or upgrade. If you have existing agents you want to protect, you must remove the agent and then reinstall the agent with the password.

Passwords are generated using the UninstallPwdKeyGenerator.exe tool.

See "Creating passwords with the password generation tool" on page 82.

You can add the uninstallation password by including the password parameter in the agent installation command line. You can use either Symantec Management Platform (SMP) or a software management system (SMS) program to install the agents with the uninstallation password.

See "About Symantec DLP Agent Installation" on page 75.

You cannot add the uninstallation password to agents through the installation wizard.

To add the uninstallation password to an agent installation

- Add the uninstallation password parameter in the agent installation command line

  `UNINSTALLPASSWORDKEY="<password key>"`

  where `<password key>` is the password that you created with the password generation tool.

A sample agent installation command line might look like the following example:

```
msiexec /i AgentInstall.msi /q
INSTALLDIR="%ProgramFiles%\Manufacturer\Endpoint Agent\"
ENDPOINTSERVER="hostname" PORT="8000" KEY="" UNINSTALLPASSWORDKEY=
"<password key>" SMC="hostname" SERVICENAME="EDPA" WATCHDOGNAME="WDP"
```

See "Using uninstallation passwords" on page 83.

Using uninstallation passwords

When you want to uninstall a Symantec 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 computer that requests the password. You must enter the password in this window. If you are using a software management system, include the password parameter in the command string.

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 "Creating passwords with the password generation tool" on page 82.

See "About uninstallation passwords" on page 81.

Upgrading agents and uninstallation passwords

You can upgrade any agents which are protected by uninstallation passwords without affecting the password. If you do not want to change the password, do not include the password parameter to the upgrade command line. The pre-existing uninstallation password is included in the upgraded agent automatically. Only include the password parameter if you want to change the password or if you want to add a new password to an agent.

To add or change a password while upgrading an agent

- Add the following password parameter to the upgrade command line:

  `UNINSTALLPASSWORDKEY=<password key>`

  where `<password key>` is the password key that you created using the password generation tool.

See "Creating passwords with the password generation tool" on page 82.

See "About uninstallation passwords" on page 81.

Installing Symantec DLP Agents with an unattended installation

You can use an unattended installation process by using a systems management software product (SMS) to install Symantec DLP Agents to endpoint computers. You must always install the AgentInstall.msi package from a local directory. If you do not install from a local directory, some functions of the Symantec DLP Agent are disabled.

To perform an unattended installation

1. In your systems management software package, specify the AgentInstall.msi or AgentInstall64.msi package.
2. Specify the AgentInstall.msi installation properties.

   See "About the AgentInstall.msi package" on page 80.
3. Specify the `msiexec` properties.

   Optional properties for the `msiexec` utility.

   See "About the AgentInstall.msi package" on page 80.
4. Specify any optional properties for the `msiexec` utility.

   See "About the AgentInstall.msi package" on page 80.

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

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

```
msiexec /i AgentInstall.msi /q INSTALLDIR="C:\Program
    Files\Manufacturer\Symantec DLP Agent\" ARPSYSTEMCOMPONENT="1"

ENDPOINTSERVER="epserver:8001"

SERVICENAME="ENDPOINT" WATCHDOGNAME="WATCHDOG"
```

In this command:

`msiexec` is the Windows command for executing MSI packages.

`/i` specifies the name of the package.

`/q` specifies a silent install.

`INSTALLDIR` and `ARPSYSTEMCOMPONENT` are optional properties to `msiexec`.

`ENDPOINTSERVER`, `SMC`, `SERVICENAME`, and `WATCHDOGNAME` are properties for the AgentInstall.msi package.

Symantec Data Loss Prevention includes an example installation command in *`install_dir`*`\Endpoint\install_agent.bat`.

After you install the agents, the Symantec DLP Agent service automatically starts on each endpoint computer. 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).

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

Note: Some aspects of the Symantec DLP Agent installation may require you to restart the endpoint computer.

Installing Symantec DLP Agents manually

You can install Symantec DLP Agents manually on your endpoints by using the AgentInstall.msi or AgentInstall64.msi (for Windows 7 64-bit platforms) package.

To install Symantec DLP Agent manually

1. Log on to the endpoint computer as an administrator.
2. Copy the AgentInstall.msi or AgentInstall64.msi file to the endpoint computer and double-click the file.

   The Symantec DLP Agent installation wizard starts up, displaying the Symantec DLP Agent setup panel.
3. Click **Next** to accept the copyright agreement.
4. Click **Next** to accept the license agreement.

   Note: If your computer is not already running Windows Installer 3.1, the Symantec DLP Agent installer initiates the installation of that program. In this case, you are prompted to restart the computer after the Windows Installer installation. Upon restart, the Symantec DLP Agent installer resumes.

5. Type the appropriate values in the following fields:

   - Endpoint Servers (required)
     Enter the hostname or IP address of at least one Endpoint Server. For example, server.company.com. This value must be consistent with the **Agent Listener > Bind Address (Host/IP)** value you set for the Endpoint Server on the **Symantec Data Loss Prevention Enforce Server > Configure Server page**. If you use a non-default port number, specify it after the server name. For example, server.company.com:8001.

Note: You can specify more than four Endpoint Servers. To do so, use any of the four available text fields to enter a list of hostnames or IP addresses separated by semicolons. For example, "epserver1.company.com; epserver2.company.com; epserver3.company.com; epserver4.company.com; 10.67.20.36:8002."

- Encryption Key (optional)
  You may enter a custom authentication key that the Symantec DLP Agents and Endpoint Server use to establish a secure connection. Agents include a default authentication key, but you can also create your own key using the `endpointkeytool` utility. To use your own key, specify it with the `KEY` parameter during deployment and installation. If you decide to use a custom key after installing Symantec DLP Agents, you must reinstall the Symantec DLP Agents to specify the key.
- DLP Agent Service Name (optional)
  You may edit the Symantec DLP Agent service name that appears in the service list of the endpoint computer.
- DLP Watchdog Service Name (optional)
  You may edit the watchdog service name that appears in the service list of the endpoint computer.

6 Click **Next**.

7 Accept the default installation directory or enter a new one, and then click **Next**.

  The default is `c:\Program Files\Manufacturer\Endpoint Agent`.

8 On the Confirm Installation screen that appears, click **Install**.

  The installation takes a few moments. When it finishes, the Installation Complete screen appears.

9 Click **Finish**.

10 Go to **Start > Control Panel > Administrative Tools**, and then double-click **Services**. Find the Symantec DLP Agent service (listed under the name you typed in the Service Name field during installation). Make sure that it is running.

  The Symantec DLP Agent now monitors the endpoint.

11 Log on to the Enforce Server and go to **System > Agents > Overview**.

12 Verify that the Symantec DLP Agent is registered (appears in the list).

Chapter 8

Implementing Symantec DLP Agent management

This chapter includes the following topics:

About the Symantec Management Console

A Symantec Data Loss Prevention installation that includes Endpoint Discover or Endpoint Prevent can optionally use the Symantec Management Console for endpoint management. The Symantec Management Console (SMC) is part of the Symantec Management Platform, and it provides a centralized way for you to manage your Symantec DLP Agent installations, upgrades, and uninstallations. Using SMC, you can find all of the endpoint computers in your organization and add them to the SMC for management. You can also create your own organizational structure or use a predefined structure such as Active Directory (AD). The Symantec Management Console contains troubleshooting tools that let you investigate your Symantec DLP Agents in case there is a problem.

Note: Installing and using the Symantec Management Console with Symantec Data Loss Prevention is optional. You do not need to use the Symantec Management Console to protect your data. However, the Symantec Management Console offers several tools and capabilities that are not otherwise available in Symantec Data Loss Prevention.

See the *Symantec Data Loss Prevention Administration Guide* for information about other ways to manage endpoint computers for Endpoint Discover and Endpoint Prevent.

Symantec Management Console uses single sign-on (SSO) technology. You do not have to maintain separate credentials for Symantec Data Loss Prevention and Symantec Management Console.

For additional information about the Symantec Manage Platform, refer to the following documentation:

- "Installing the Symantec Management Platform Products," available on SymWISE at http://www.symantec.com/docs/HOWTO9795. This article provides an overview and steps for installing the Symantec Installation Manager (SIM) and the Symantec Management Platform (SMP).
- The *Symantec Management Platform Installation Guide* is available at http://go.symantec.com/sim_doc. It contains information about installing the infrastructure that enables the installation of the Data Loss Prevention Integration Component.
- The *Symantec Management Platform User's Guide* contains information about configuring the infrastructure components, for example, setting roles and privileges. After installation, you can refer to the help within the Symantec Management Platform.

Installing the Data Loss Prevention Integration Component

Use Symantec Installation Manager to install the Data Loss Prevention Integration Component and dependent products. When you select the Data Loss Prevention Integration Component to install, dependent products such as the Symantec Management Platform are selected automatically.

See "Installing the Symantec Management Platform Products" on SymWISE at http://www.symantec.com/docs/HOWTO9795. This article provides an overview and basic steps for installing the Symantec Installation Manager (SIM) and the Symantec Management Platform (SMP). Additional information is provided by

the *Symantec Management Platform Installation Guide*, which is available at http://go.symantec.com/sim_doc.

The Data Loss Prevention Integration Component is available on the Install New Products page of Symantec Installation Manager. You may need to select **All** in the "**Filter by**" menu to display and select the component.

An Internet connection is required to obtain the Symantec Installation Manager product list and download product installation files. To install products on a computer that has no Internet connection, you must create an installation package.

To install and enable automated asset discovery and endpoint installation of the Symantec DLP Agent, complete the following process after you have installed the Enforce Server:

Table 8-1 Implementation of Symantec DLP Agent Endpoint management

Step	Action	Description
Step 1	Verify that all system requirements are met for the Symantec Management Platform. The Symantec Management Platform (SMP) can be installed on the system that hosts the Endpoint Server or on a separate system.	See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*. Altiris 6 users must first upgrade to Symantec Management Platform 7 and migrate existing management data. Install Symantec Data Loss Prevention and the Data Loss Prevention Integration Component only after you have completed the upgrade. For more information, see "Installing the Symantec Management Platform Products" on SymWISE at http://www.symantec.com/docs/HOWTO9795.
Step 2	Install the Symantec Installation Manager.	The Symantec Installation Manager manages the installation of the Symantec Management Platform and solutions. See the *Symantec Management Platform Installation Guide* for instructions to install the software. Symantec Data Loss Prevention provides the Symantec Installation Manager installer application in the ZIP file: `DLPDownloadHome\DLP\Symantec_DLP_11_Win\11.6_Win\Endpoint\SymantecDLPWinAgentMgmt_11.6.zip` **Note:** The Symantec Management Platform can only be installed on Windows systems. You cannot install Symantec Management Platform on a Linux system.

Table 8-1 Implementation of Symantec DLP Agent Endpoint management *(continued)*

Step	Action	Description
Step 3	Install the Data Loss Prevention Integration Component.	Use the Symantec Installation Manager to install the Data Loss Prevention Integration Component. For more information, see "Installing the Symantec Management Platform Products" on SymWISE at http://www.symantec.com/docs/HOWTO9795. **Note:** Do not perform asset discovery or select computers in the **Computers to Manage** window during the installation process. Perform asset discovery only after you have installed all Symantec Data Loss Prevention products.
Step 4	Configure the Symantec Management Platform.	Define roles and permissions for Symantec DLP Agent management. See "Configuring the Symantec Management Platform for use with the Integration Component" on page 92.
Step 5	Enter the host name or IP address of the Symantec Management Platform Console in the Enforce Server administration console.	
Step 6	From the Data Loss Prevention Portal, perform computer (asset) discovery of the endpoints.	See the information about computer discovery in the *Symantec Data Loss Prevention Administration Guide*.
Step 7	Deploy the Altiris Agent and the Symantec DLP Agent to the endpoints, and verify the deployment.	See the *Symantec Data Loss Prevention Administration Guide*.

Configuring the Symantec Management Platform for use with the Integration Component

After you install the Symantec Management Platform, configure it for optimal use with the Data Loss Prevention Integration Component.

Configuring security roles and permissions is optional, but recommended.

For security roles and permissions, use the guideline of least privilege. Test your selected roles to make sure you have the right access permissions.

For more information about configuring Symantec Management Platform security roles, see the *Symantec Management Platform User's Guide*.

To configure security roles and permissions

1 Log on to the Symantec Management Console.

Note: The Symantec Management Console supports NTLM authentication from remote computers (single sign-on). See the *Symantec Management Platform User's Guide* for more information.

---

2 In the Symantec Management Console, on the **Settings** menu, click **Security Roles**.

3 Create a new security role for Data Loss Prevention.

For more information, see topics on security roles in the *Symantec Management Platform User's Guide*.

4 Initially, enable all privileges under **Management Privileges**, **Symantec Management Console Privileges**, and **Right-click Menu** (except do not enable the delete privilege).

5 Disable all other privileges, unless specifically needed.

6 Click **Settings** > **Security** > **Permissions**, and then click the **Security Role Manager** tab.

7 Select the Data Loss Prevention security role.

8 In the drop-down list, select each of the different views.

9 Click the edit icon to edit permissions, and add the permissions that are required for the role.

10 Test the selected permissions.

11 Repeat these steps until you have the right access permissions for your site.

See "Installing the Data Loss Prevention Integration Component" on page 90.

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 95.

See "About system events and syslog servers" on page 115.

See "Enforce Servers and unused NICs" on page 116.

See "Performing initial setup tasks on the Enforce Server" on page 116.

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 97.

See "About Symantec DLP Agent security" on page 101.

See "Symantec Data Loss Prevention directory and file exclusion from antivirus scans" on page 105.

See "Corporate firewall configuration" on page 106.

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 97.
  See "Generating a unique browser certificate" on page 98.
- 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 45.
See "Using sslkeytool to generate new Enforce and detection server certificates" on page 47.

See "About post-installation tasks" on page 95.

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 98.

See "About server security and SSL/TLS certificates" on page 96.

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 Enforce Server services" on page 119.
3. On the Enforce Server, go to the `\Vontu\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 running 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:\Vontu\Protect\tomcat\conf` directory.
7. Restart the Vontu services on the Enforce Server.

   See "About Enforce Server services" on page 119.

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 96.

Note: If you use SPC authentication and the CA certificate for the Enforce Server is updated after your register an SPC instance, you must re-register the SPC instance. If you register an SPC instance you use a self-signed certificate for the Enforce Server, The Enforce Server automatically regenerates the certificate after the certificate expires.

About Symantec DLP Agent security

Symantec Data Loss Prevention uses Advanced Encryption Standard (AES) technology to secure communications between the Endpoint Server and the Symantec DLP Agent. Symantec Data Loss Prevention also uses AES to secure the Symantec DLP Agent database file.

AES is a symmetric-key encryption technology that supports key sizes of 128, 192, and 256 bits.

Symantec Data Loss Prevention uses the following sets of AES keys:

- One to secure the agent database file
- One to authenticate the Endpoint Server to the Symantec DLP Agent
- One to encrypt traffic between the Endpoint Server and Symantec DLP Agent

The database file key is only used at the Symantec DLP Agent. However, the authentication key and the traffic encryption keys must be shared between the Endpoint Server and Symantec DLP Agent. By default, Symantec Data Loss Prevention uses the predefined 128-bit database and authentication keys. The traffic encryption key is a randomly generated session key that is negotiated every time the Symantec DLP Agent connects to the Endpoint Server.

Although the information in Symantec Data Loss Prevention is secure, you should change the default keys. You can change the database key, the authentication key, and the AES key size (128, 192, 256). You should change these default settings (either change them to use unique keys or change the key size) before you deploy the Symantec DLP Agents. Symantec Data Loss Prevention includes the `endpointkeytool` utility to generate the authentication key. The `endpointkeytool` utility also lets you create a tools-password that you need to access the other endpoint tools.

See "About endpointkeytool utility" on page 102.

See "Running the endpointkeytool utility" on page 103.

A new traffic encryption key is randomly generated each time a Symantec DLP Agent connects to the Endpoint Server. The key is discarded as soon as the connection session between server and agent ends. The traffic encryption key is always unique for each Symantec DLP Agent connection session. The authentication key is shared in common by the Endpoint Server with all Symantec DLP Agents.

By default, Symantec Data Loss Prevention is configured to use the 128-bit key size to protect communication between the Endpoint Server and Symantec DLP Agents. However, the bit size of the authentication key can be increased to enhance encryption. If the bit size for the authentication key is increased, the bit size of the traffic encryption key is automatically increased. In this way, the two

encryption keys always have matching bit-sizes. The bit size of the authentication key can only be changed before you install Symantec DLP Agents.

About the authentication key

All Symantec Data Loss Prevention customers are provided with a default 128-bit authentication key that is hard-coded into the product. This authentication key works well for many customers, but you have the option to generate a new authentication key. Several factors need to be considered before you replace an authentication key.

The benefits of generating a new authentication key are as follows:

- A new AES key isolates you from other Symantec customers that use the default key. The default configuration is to use the authentication key that is hard-coded into Symantec Data Loss Prevention. All Symantec Data Loss Prevention customers use the same authentication key unless the key is changed.
- The encryption security for data traffic can be enhanced by increasing the size of the authentication key to 192- or 256-bit. The greater bit size makes compromising data security even more difficult.

The drawbacks to generating a new authentication key are as follows:

- Advance planning is required before the Symantec DLP Agents are installed. You cannot change the authentication key after the Agents are installed.
- The United States government regulates the use of 192-bit and 256-bit AES keys. Export laws highly restrict the use of these keys outside of the United States. System performance may also suffer by using larger key sizes.

You can change the authentication key with the `endpointkeytool` utility.

See "About endpointkeytool utility" on page 102.

See "Running the endpointkeytool utility" on page 103.

About endpointkeytool utility

Use the endpointkeytool command-line utility to generate an authentication key and define a tools password. Symantec Data Loss Prevention uses default keys. You must generate your own unique keys to ensure that you do not use the same key as another customer. Back up and secure the files that the endpointkeytool generates. Before you start, make sure that the Endpoint Server is installed but that no Symantec DLP Agents are installed.

Note: Please check your operating system licensing limitations as some key sizes are not recognized outside of the United States.

See "Running the endpointkeytool utility" on page 103.

See "About Symantec DLP Agent security" on page 101.

Running the endpointkeytool utility

The endpointkeytool utility must run under the Symantec Data Loss Prevention operating system user account. By default the account is "protect." The command options for the endpointkeytool utility are:

Option	Description
`-keysize=<128/192/256>`	Specifies the bit-size of the generated key file.
`-pwd=`*`tools_password`*	Specifies the password to access the endpoint tools. By default, the password is *VontuStop*. You must specify a password.
`[-dir=`*`directory`*`]`	The optional `-dir` argument specifies the directory where the keystore files are placed.

Unless you specified a different directory with the `-dir` argument, the keystore file *.endpointRecoveryStore is created in the `\bin` directory where the endpointkeytool utility resides. By default, the `\bin` directory is `...Enforce\Protect\bin`. This keystore file must be moved to the keystore directory to function.

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

To generate an endpointkeytool file

1 Under the Symantec Data Loss Prevention user account, run the `endpointkeytool` utility with the needed parameters, for example:

```
endpointkeytool generate -keysize=128 -pwd=VontuStop
```

2. Enter a tools password using the parameters `-pwd=tools_password` and `-keysize=128/192/256`. In the command, `tools_password` is the password you want to use and `128/192/256` is the size of the key you want to use.
3. Unless you used the `-dir` option to specify where the keystore file is generated, place the keystore file in a safe, memorable directory. Verify that the keystore directory contains only one keystore file.
4. Store a copy of the keystore file in a safe location. If anything happens to the keystore file on a Symantec DLP Agent, a copy of the keystore file is available to replace the damaged file.

   The Endpoint Server must use the key that is generated at the same `endpointkeytool` session. Any Symantec DLP Agent that uses a different key cannot be authenticated and cannot communicate with the server. An Authentication Failure Endpoint system event is generated if a problem with the keystore file occurs. The Symantec DLP Agent status is shown in the Agent Overview screen of the management console.
5. Copy the authentication key into the `KEY` parameter for the MSI installation script for installing Symantec DLP Agents. This procedure ensures that the installation script installs all Symantec DLP Agents with the same authentication key. If the `KEY` parameter is left empty, then the Symantec DLP Agents use the default key.

   The Endpoint Server has a keystore directory that is located at `Vontu/Protect/keystore`. An empty keystore directory indicates that Symantec Data Loss Prevention is using the default embedded keystore file. After the generated keystore file is copied into the keystore directory, it overrides the default keystore file.

   If you forget your tools password, you can recover it using the endpointkeytool recover option:

   ```
   endpointkeytool recover [-dir=output_dir]
   ```
6. Restart the Endpoint Server through the Enforce console.

See "About Symantec DLP Agent security" on page 101.

See "About endpointkeytool utility" on page 102.

See "About the authentication key" on page 102.

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 105.

See "Oracle directory and file exclusion from antivirus scans" on page 106.

See "About post-installation tasks" on page 95.

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:

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

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

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

- `\Vontu\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 104.

See "Oracle directory and file exclusion from antivirus scans" on page 106.

See "About post-installation tasks" on page 95.

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\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 104.

See "Symantec Data Loss Prevention directory and file exclusion from antivirus scans" on page 105.

See "About post-installation tasks" on page 95.

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 or OracleOraDb10g_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)
- Vontu Incident Persister (for Enforce Server only)
- Vontu Manager (for Enforce Server only)
- Vontu Monitor (for detection servers only)
- Vontu Notifier (for Enforce Server only)
- Vontu Update
- 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
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
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

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

User rights assignment	Recommended security settings
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	
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

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

User rights assignment	Recommended security settings
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
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

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

Security options	Recommended security settings
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
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

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

Security options	Recommended security settings
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
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

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

Security options	Recommended security settings
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 95.

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 `\Vontu\Protect\config\model.properties` file:

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

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

```
model.notification.host=IP
\Vontu\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. If you chose to use SPC authentication or certificate authentication, you must finish configuring those authentication mechanisms after installation.

4 Add an email address for the Administrator user account so you can be notified of system events.

5 Add user accounts for all users who are authorized to use the system, and provide them with their log on information.

6 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.

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

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

9 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 Enforce Server 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 Services on the Enforce Server

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

Table 10-1 Services on the Enforce Server *(continued)*

Service Name	Description
Vontu Update	Installs the Symantec Data Loss Prevention system updates. This service only runs during system updates and upgrades.

See "About starting and stopping services on Windows" on page 120.

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 120.
- See "Stopping an Enforce Server on Windows" on page 121.
- See "Starting a Detection Server on Windows" on page 121.
- See "Stopping a Detection Server on Windows" on page 121.
- See "Starting services on single-tier Windows installations" on page 122.
- See "Stopping services on single-tier Windows installations" on page 122.

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. Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
3. Start the remaining Symantec Data Loss Prevention services, including the following services:
   - Vontu Manager
   - Vontu Incident Persister
   - Vontu Update
   - Vontu Monitor Controller

See "Stopping an Enforce Server on Windows" on page 121.

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, which might include the following services:
   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor Controller
   - Vontu Notifier

See "Starting an Enforce Server on Windows" on page 120.

Starting a Detection Server on Windows

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

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

See "Stopping a Detection Server on Windows" on page 121.

Stopping a Detection Server on Windows

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

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

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

See "Starting a Detection Server on Windows" on page 121.

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. Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
3. Start the remaining Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Manager
   - Vontu Monitor
   - Vontu Incident Persister
   - Vontu Update
   - Vontu Monitor Controller

See "Stopping services on single-tier Windows installations" on page 122.

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, which might include the following services:
   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor Controller
   - Vontu Notifier
   - Vontu Monitor

See "Starting services on single-tier Windows installations" on page 122.

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. 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.

2. Click **Next** to display the **Preserve CryptoMasterKey.properties** panel.

3. Select **Preserve CryptoMasterKey.properties** to indicate that the uninstaller should not remove the `CryptoMasterKey.properties` file.

   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.

   ---

4. Click **Next** to uninstall Symantec Data Loss Prevention.

5. Click **Finish** to complete the uninstall process.

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

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 install FIPS, 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 128.

Note: You must install all Symantec Data Loss Prevention servers with the same encryption option; you cannot mix encryption options.

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 128.

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 127.

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:

  ```
  ProtectInstaller_11.6.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 29.

  See "Installing a detection server" on page 57.

  See "Installing a single-tier server" on page 63.

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 128.

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

H

I

K

L

M

N

O

P

R

S

T

U

V

W