

Symantec™ Data Loss Prevention Installation Guide for Linux

Version 11.0



Symantec Data Loss Prevention Installation Guide for Linux

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 11.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third-Party License Agreements* document accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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

| | | |
|-------------------------|---|----|
| Technical Support | 4 | |
| Chapter 1 | Planning the Symantec Data Loss Prevention installation | 11 |
| | About installation tiers | 11 |
| | About 64-bit operating system support | 12 |
| | About hosted Network Prevent deployments | 13 |
| | About Symantec Data Loss Prevention system requirements | 13 |
| | Symantec Data Loss Prevention required materials | 14 |
| | Standard ASCII characters required for all installation parameters | 15 |
| | Performing a three-tier installation—high-level steps | 15 |
| | Performing a two-tier installation—high-level steps | 18 |
| | Performing a single-tier installation—high-level steps | 20 |
| | Symantec Data Loss Prevention preinstallation steps | 21 |
| | Verifying that servers are ready for Symantec Data Loss Prevention installation | 23 |
| Chapter 2 | Installing an Enforce Server | 25 |
| | Installing an Enforce Server | 25 |
| | Verifying an Enforce Server installation | 30 |
| Chapter 3 | Importing a solution pack | 33 |
| | About Symantec Data Loss Prevention solution packs | 33 |
| | Importing a solution pack | 34 |
| Chapter 4 | Configuring certificates for secure communication | 37 |
| | About the sslkeytool utility and server certificates | 37 |
| | About sslkeytool command line options | 38 |
| | Using sslkeytool to generate new Enforce and detection server certificates | 39 |
| | Using sslkeytool to add new detection server certificates | 41 |

| | | |
|-----------|--|----|
| | Verifying server certificate usage | 43 |
| Chapter 5 | Installing and registering detection servers | 45 |
| | About detection servers | 45 |
| | Detection servers and remote indexers | 47 |
| | Detection server installation preparations | 48 |
| | Installing a detection server | 48 |
| | Verifying a detection server installation | 51 |
| | Registering a detection server | 51 |
| Chapter 6 | Performing a single-tier installation | 55 |
| | Installing a single-tier server | 55 |
| | Verifying a single-tier installation | 59 |
| Chapter 7 | Implementing Symantec DLP Agent management | 61 |
| | About implementing Symantec DLP Agent endpoint management | 61 |
| | Installing the Data Loss Prevention Integration Component | 62 |
| | Configuring the Symantec Management Platform for use with the Integration Component | 64 |
| Chapter 8 | Post-installation tasks | 67 |
| | About post-installation tasks | 67 |
| | About post-installation security configuration | 67 |
| | About server security and SSL/TLS certificates | 68 |
| | About Symantec DLP Agent security | 72 |
| | About Symantec Data Loss Prevention and antivirus software | 76 |
| | Corporate firewall configuration | 78 |
| | About system events and syslog servers | 79 |
| | Performing initial setup tasks on the Enforce Server | 79 |
| Chapter 9 | Starting and stopping Symantec Data Loss Prevention services | 81 |
| | About Enforce Server services | 81 |
| | Starting and stopping services on Linux | 82 |
| | Starting an Enforce Server on Linux | 82 |
| | Stopping an Enforce Server on Linux | 83 |
| | Starting a detection server on Linux | 83 |

| | | |
|-------------|---|----|
| | Stopping a detection server on Linux | 83 |
| | Starting services on single-tier Linux installations | 84 |
| | Stopping services on single-tier Linux installations | 84 |
| Chapter 10 | Uninstalling Symantec Data Loss Prevention | 87 |
| | Uninstalling a server from a Linux system | 87 |
| Appendix A | Installing Symantec Data Loss Prevention with the FIPS encryption option | 89 |
| | About FIPS encryption | 89 |
| | Installing Symantec Data Loss Prevention with FIPS encryption enabled | 90 |
| | Configuring Internet Explorer when using FIPS | 90 |
| Index | | 93 |

Planning the Symantec Data Loss Prevention installation

This chapter includes the following topics:

- [About installation tiers](#)
- [About 64-bit operating system support](#)
- [About hosted Network Prevent deployments](#)
- [About Symantec Data Loss Prevention system requirements](#)
- [Symantec Data Loss Prevention required materials](#)
- [Standard ASCII characters required for all installation parameters](#)
- [Performing a three-tier installation—high-level steps](#)
- [Performing a two-tier installation—high-level steps](#)
- [Performing a single-tier installation—high-level steps](#)
- [Symantec Data Loss Prevention preinstallation steps](#)
- [Verifying that servers are ready for Symantec Data Loss Prevention installation](#)

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 | <p>To implement the single-tier installation, you install the database, the Enforce Server, and a detection server all on the same computer.</p> <p>Use single-tier installation only for testing or risk assessment purposes.</p> <p>See “Performing a single-tier installation—high-level steps” on page 20.</p> |
| Two-tier | <p>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 database administration team.</p> <p>If you choose this installation, the administrator needs to be able to perform database maintenance tasks, such as database backups.</p> <p>See “Performing a two-tier installation—high-level steps” on page 18.</p> |
| Three-tier | <p>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.</p> <p>See “Performing a three-tier installation—high-level steps” on page 15.</p> |

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 executable for your platform. Using the correct installer copies the required 64-bit JVM and 64-bit executables, and configures the server for 64-bit operating systems.

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 via 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 (Email) and Network Prevent (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.

See [“Installing a detection server”](#) on page 48.

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 39.

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 *DLPSDownloadHome* 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 an Endace card for packet capture.
- **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).
- **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, `/opt/'symantec products'/Vontu` is not a valid installation folder.

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 21. |
| Step 2 | Verify that your servers are ready for installation. | See “Verifying that servers are ready for Symantec Data Loss Prevention installation” on page 23. |

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

| Step | Action | Description |
|--------|--|--|
| Step 3 | Install Oracle and create the Symantec Data Loss Prevention database. | <p>In a three-tier installation your organization's database administration team installs, creates, and maintains the Symantec Data Loss Prevention database.</p> <p>See the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i> for information about installing Oracle.</p> |
| Step 4 | Install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server computer to enable communication with the Oracle server. | <p>The user account that is used to install Symantec Data Loss Prevention requires access to SQL*Plus to create tables and views.</p> <p>See the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i> for information about installing the Oracle client software.</p> |
| Step 5 | Install the Enforce Server. | See “Installing an Enforce Server” on page 25. |
| Step 6 | Verify that the Enforce Server is correctly installed. | See “Verifying an Enforce Server installation” on page 30. |
| Step 7 | Import a solution pack. | <p>See “Importing a solution pack” on page 34.</p> <p>See “About Symantec Data Loss Prevention solution packs” on page 33.</p> |

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

| Step | Action | Description |
|---------|--|---|
| Step 8 | Generate server certificates for secure communication. | <p>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.</p> <p>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.</p> <p>See “Using sslkeytool to generate new Enforce and detection server certificates” on page 39.</p> |
| Step 9 | If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, implement and configure the Symantec Management Platform (SMP) for Endpoint management and then enter the SMP address in the Enforce Server administration console. | See “About implementing Symantec DLP Agent endpoint management” on page 61. |
| Step 10 | Install a detection server. | See “Installing a detection server” on page 48. |
| Step 11 | Register a detection server. | See “Registering a detection server” on page 51. |
| Step 12 | Perform the post-installation tasks. | See “About post-installation tasks” on page 67. |

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

| Step | Action | Description |
|---------|---|--|
| 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 67. For more detailed administration topics (including how to configure a specific detection server) see the <i>Symantec Data Loss Prevention Administration Guide</i> . |

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 21. |
| Step 2 | Verify that your servers are ready for installation. | See “Verifying that servers are ready for Symantec Data Loss Prevention installation” on page 23. |
| Step 3 | Install Oracle and create the Symantec Data Loss Prevention database. | See the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i> . |
| Step 4 | Install the Enforce Server. | See “Installing an Enforce Server” on page 25. |
| Step 5 | Verify that the Enforce Server is correctly installed. | See “Verifying an Enforce Server installation” on page 30. |

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

| Step | Action | Description |
|---------|--|--|
| Step 6 | Import a solution pack. | See “Importing a solution pack” on page 34. See “About Symantec Data Loss Prevention solution packs” on page 33. |
| 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 39. |
| Step 8 | If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, implement and configure the Symantec Management Platform (SMP) for Endpoint management and then enter the SMP address in the Enforce Server administration console. | See “About implementing Symantec DLP Agent endpoint management” on page 61. |
| Step 9 | Install a detection server. | See “Installing a detection server” on page 48. |
| Step 10 | Register a detection server. | See “Registering a detection server” on page 51. |

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

| Step | Action | Description |
|---------|---|--|
| Step 11 | Perform the post-installation tasks. | See “About post-installation security configuration” on page 67. |
| 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 67. For more detailed administration topics (including how to configure a specific detection server) see the <i>Symantec Data Loss Prevention Administration Guide</i> . |

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 21. |
| Step 2 | Verify that the server is ready for installation. | See “Verifying that servers are ready for Symantec Data Loss Prevention installation” on page 23. |
| Step 3 | Install Oracle and create the Symantec Data Loss Prevention database. | See the <i>Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide</i> . |

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

| Step | Action | Description |
|--------|--|--|
| Step 4 | Install the Enforce Server and a detection server on the same computer. | See “Installing a single-tier server” on page 55. |
| Step 5 | Verify that the Enforce Server is correctly installed. | See “Verifying a single-tier installation” on page 59. |
| Step 6 | Import a solution pack. | See “About Symantec Data Loss Prevention solution packs” on page 33. See “Importing a solution pack” on page 34. |
| Step 7 | If your Symantec Data Loss Prevention installation includes Endpoint Discover or Endpoint Prevent, implement and configure the Symantec Management Platform (SMP) for Endpoint management and then enter the SMP address in the Enforce Server administration console. | See “About implementing Symantec DLP Agent endpoint management” on page 61. |
| Step 8 | Register the detection server. | See “Registering a detection server” on page 51. |
| 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 67. For more detailed administration topics (including how to configure a specific detection server) see the <i>Symantec Data Loss Prevention Administration Guide</i> . |

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 13.
- You have gathered the required materials.

See [“Symantec Data Loss Prevention required materials”](#) on page 14.

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 Obtain the root password for each Symantec Data Loss Prevention server.
- 3 Obtain the static IP address(es) for each system on which Symantec Data Loss Prevention is to be installed.
- 4 Verify that each server hostname that you will specify has a valid DNS entry.
- 5 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).
- 6 Copy the following files from *DLPDownloadHome* to an easily accessible directory on the Enforce Server:
 - The Symantec Data Loss Prevention installer: `ProtectInstaller_11.0.sh` for 32-bit platforms or `ProtectInstaller64_11.0.sh` for 64-bit platforms. This file can be found in the *DLPDownloadHome/DLP/11.0_Lin/New_Installs* directory.
 - 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/11.0_Lin/Solution_Packs* directory. See [“About Symantec Data Loss Prevention solution packs”](#) on page 33.
 - 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_11.0.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/11.0_Lin/New_Installs* directory.

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

- 7 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.
 - 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 an Endace card, then do not set this port up for SPAN or tap.
- 3 Log on as the superuser.
- 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 Internet protocol TCP/IP enabled. Disabling any of this can cause communication problems between the Enforce Server and the detection servers.
- 6 Use `ifconfig` to verify all assigned IP addresses.
- 7 If you are using DNS, verify that all hostnames have valid DNS entries.
- 8 Ping each Symantec Data Loss Prevention server computer (using both IP and hostname) to verify network access.
- 9 Verify that ports 443 (SSL) and 3389 (RDP) are open and accessible to the client computers that require access.
- 10 Verify that port 25 is not blocked. The Symantec Data Loss Prevention server uses port 25 (SMTP) for email alerts.
- 11 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.

See [“Symantec Data Loss Prevention required materials”](#) on page 14.

See [“Symantec Data Loss Prevention preinstallation steps”](#) on page 21.

For a Network Prevent (Email) 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 (Email) Server computer to the MTA on port 25. Also ensure that you can Telnet from the MTA to the Network Prevent (Email) Server computer on port 10026.

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

Installing an Enforce Server

This chapter includes the following topics:

- [Installing an Enforce Server](#)
- [Verifying an Enforce Server installation](#)

Installing an Enforce Server

The instructions that follow describe how to install an Enforce Server. These instructions are not required if you have already installed a single-tier installation (which includes the Enforce Server component).

Before installing an Enforce Server:

- Complete the preinstallation steps.
See [“Symantec Data Loss Prevention preinstallation steps”](#) on page 21.
- Verify that the system is ready for installation.
See [“Verifying that servers are ready for Symantec Data Loss Prevention installation”](#) on page 23.
- 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.

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 89.

Note: The following instructions assume that the `ProtectInstaller_11.0.sh` or `ProtectInstaller64_11.0.sh` file, license file, and solution pack file have been copied into the `/opt/temp` directory on the Enforce Server.

To install an Enforce Server

- 1 Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Loss Prevention installation process.
- 2 Log on as root to the Enforce Server system on which you intend to install Enforce.
- 3 Go to the directory where you copied the `ProtectInstaller_11.0.sh` or `ProtectInstaller64_11.0.sh` file (`/opt/temp/`) and run the installer, by entering:

```
./ProtectInstaller_11.0.sh
```

If your system does not support a graphical user interface, run the installer by typing `-c` after the file name. For example:

```
./ProtectInstaller_11.0.sh -c
```

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

- 4 Click **Next**.
The **License Agreement** appears.
- 5 After reviewing the license agreement, select **I accept the agreement**, and click **Next**.

The **Select Components** panel appears.

- 6 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.

■ **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.

■ **Indexer**

Select **Indexer** to install a remote indexer.

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

The **License File** panel appears.

- 7 Browse to the directory containing your license file. Select the license file, and click **Next**.

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

The **Select Destination Directory** panel appears.

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

```
/opt/Vontu
```

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.

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

- 9 In the **Select Directory for Symlinks** panel, select one of the following options and then click **Next**.
 - If you want to use symbolic links with Symantec Data Loss Prevention, enter a Destination directory. Symbolic links let you run a program without having to specify the entire path. The default is `/usr/local/bin`. However, you can click **Browse** to navigate to a different location.

- Otherwise, select **Don't create symlinks**.

- 10 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.

The **Administrator Password** panel appears.

- 11 Enter the Administrator user account password to access the Enforce Server administration console, and confirm the password. Then click **Next**.

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.

The **Symantec Management Console** panel appears.

- 12 In the **Symantec Management Console** panel, enter the host name or IP address of the Symantec Management Console server for Symantec Data Loss Prevention Endpoint Agents, and click **Next**.

See ["About implementing Symantec DLP Agent endpoint management"](#) on page 61.

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.

The **Oracle Database Server Information** panel appears.

- 13 Enter the location of the Oracle Base and Home directories.

- The default Base directory is `/opt/oracle`.
- The default Home directory is `/opt/oracle/product/11.2.0/db_1`

Note that both of these are directories on the Enforce Server, not directories on a separate Oracle server (three-tier installation).

- 14 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.

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

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

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.

The **Final Confirmation** panel appears.

17 Select one of the following options in the **Final Confirmation** 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. Note that skipping the database initialization process leaves the existing Administrator password unchanged.

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.

- 18 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.

- 19 Click **Finish**.

For Linux systems, setting the ownership and permission of Symantec Data Loss Prevention files may take several minutes. The installation program window may persist for a while, during the startup of the services.

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

- 21 Verify that the Enforce Server is properly installed.

See [“Verifying an Enforce Server installation”](#) on page 30.

- 22 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 33.

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.

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
`/opt/Vontu/.install4j/installation.log`. Also
`/var/log/Vontu/*.logs`.
 - Symantec Data Loss Prevention operational logs are in `/var/log/Vontu`.
 - Oracle logs can be found in `/opt/oracle/product/10.2.0/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.

Importing a solution pack

This chapter includes the following topics:

- [About Symantec Data Loss Prevention solution packs](#)
- [Importing a solution pack](#)

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_v11.0.vsp`).

Solution pack files are stored in `DLPDownloadHome`
`/DLP/Symantec_DLP_11.0_Lin/11.0_Lin/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_EV_v11.0.vsp |
| Energy & Utilities Solution Pack | Energy_v11.0.vsp |
| EU and UK Solution Pack | EU_UK_v11.0.vsp |
| Federal Solution Pack | Federal_v11.0.vsp |
| Financial Services | Financial_v11.0.vsp |
| Health Care Solution Pack | Health_Care_v11.0.vsp |

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

| Name | File name |
|-------------------------------------|-------------------------------|
| High Tech Solution Pack | High_Tech_v11.0.vsp |
| Insurance Solution Pack | Insurance_v11.0.vsp |
| Manufacturing Solution Pack | Manufacturing_v11.0.vsp |
| Media & Entertainment Solution Pack | Media_Entertainment_v11.0.vsp |
| Pharmaceutical Solution Pack | Pharmaceutical_v11.0.vsp |
| Retail Solution Pack | Retail_v11.0.vsp |
| Telecom Solution Pack | Telecom_v11.0.vsp |
| Vontu Classic | Vontu_Classic_v11.0.vsp |

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

Solution pack documentation can be found in the `DLPDownloadHome` /DLP/Symantec_DLP_11.0_Lin/11.0_Lin/Docs/SolutionPacks directory that 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 34.

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 11.0 Enforce Server.

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

To import a solution pack

- 1 Decide which solution pack you want to use.

See [“About Symantec Data Loss Prevention solution packs”](#) on page 33.

Note: You must use a version 11.0 solution pack; earlier versions are not supported.

- 2 Log on as root to the Enforce Server computer.
- 3 Copy the solution pack file from *DLPDownloadHome*
/DLP/Symantec_DLP_11.0_Lin/11.0_Lin/Solution_Packs/ to an easily accessible local directory.
- 4 From the command-line prompt, change directory to
/opt/Vontu/Protect/bin.

```
cd /opt/Vontu/Protect/bin
```

- 5 Stop all Symantec Data Loss Prevention services except for the Notifier service, by entering the following commands:

```
./VontuUpdate.sh stop
```

```
./VontuIncidentPersister.sh stop
```

```
./VontuManager.sh stop
```

```
./VontuMonitor.sh stop (if a single-tier installation)
```

```
./VontuMonitorController.sh stop
```

The Notifier service must remain running.

See [“About Enforce Server services”](#) on page 81.

- 6 Import the solution pack by running `SolutionPackInstaller` 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_v11.0.vsp` solution pack in the `/opt/Vontu` directory of the Enforce Server, you would enter:

```
./SolutionPackInstaller import /opt/Vontu/Financial_v11.0.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:

See [“About Enforce Server services”](#) on page 81.

- 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.
- On a single-tier installation register a detection server.
See [“Registering a detection server”](#) on page 51.

Configuring certificates for secure communication

This chapter includes the following topics:

- [About the sslkeytool utility and server certificates](#)
- [About sslkeytool command line options](#)
- [Using sslkeytool to generate new Enforce and detection server certificates](#)
- [Using sslkeytool to add new detection server certificates](#)
- [Verifying server certificate usage](#)

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 38.

See [“Using `sslkeytool` to generate new Enforce and detection server certificates”](#) on page 39.

See [“Using `sslkeytool` to add new detection server certificates”](#) on page 41.

See [“About server security and SSL/TLS certificates”](#) on page 68.

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 `\Vontu\Protect\bin` directory (Windows) or `/opt/Vontu/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 37.

See [“Using `sslkeytool` to generate new Enforce and detection server certificates”](#) on page 39.

See [“Using `sslkeytool` to add new detection server certificates”](#) on page 41.

See [“About server security and SSL/TLS certificates”](#) on page 68.

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 `/opt/Vontu/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:

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

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

```
■ enforce.timestamp.sslKeyStore
■ monitor.timestamp.sslKeyStore
```

`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 `/opt/Vontu/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 `/opt/Vontu/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 41.

See [“About `sslkeytool` command line options”](#) on page 38.

See [“About the `sslkeytool` utility and server certificates”](#) on page 37.

See [“About server security and SSL/TLS certificates”](#) on page 68.

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 `/opt/Vontu/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 `/opt/Vontu/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.

Installing and registering detection servers

This chapter includes the following topics:

- [About detection servers](#)
- [Detection servers and remote indexers](#)
- [Detection server installation preparations](#)
- [Installing a detection server](#)
- [Verifying a detection server installation](#)
- [Registering a detection server](#)

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 | <p>Network Discover identifies unsecured confidential data that is exposed on open file shares and Web servers.</p> <p>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.</p> |
| Network Prevent for E-mail | <p>Network Prevent (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.</p> <p>Note: You can optionally deploy Network Prevent (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.</p> <p>See “About hosted Network Prevent deployments” on page 13.</p> |
| Network Prevent for Web | <p>Network Prevent (Web) prevents data security violations for data that is transmitted by Web communications and file-transfer protocols.</p> <p>Note: You can optionally deploy Network Prevent (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.</p> <p>See “About hosted Network Prevent deployments” on page 13.</p> |
| Endpoint Prevent | <p>Endpoint Prevent monitors the use of sensitive data on endpoint systems and detects endpoint policy violations.</p> |

Table 5-1 Detection servers (*continued*)

| Server Name | Description |
|----------------|--|
| Classification | <p>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.</p> <p>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 <i>Enterprise Vault Data Classification Services Integration Guide</i> for more information.</p> |

See [“Detection servers and remote indexers”](#) on page 47.

See [“Detection server installation preparations”](#) on page 48.

See [“Installing a detection server”](#) on page 48.

See [“Verifying a detection server installation”](#) on page 51.

See [“Registering a detection server”](#) on page 51.

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 48.

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 21.
- Verify that the system is ready for detection server installation.
See [“Verifying that servers are ready for Symantec Data Loss Prevention installation”](#) on page 23.
- Before you begin, make sure you have access and permission to run the Symantec Data Loss Prevention installer software: `ProtectInstaller_11.0.sh` for 32-bit installations or `ProtectInstaller64_11.0.sh` for 64-bit installations.

See [“Installing a detection server”](#) on page 48.

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 45.

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_11.0.sh` or `ProtectInstaller64_11.0.sh` file has been copied into the `/opt/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 48.
- 2 Log on as root to the computer that is intended for the detection server.

- 3 Copy the Symantec Data Loss Prevention installer (`ProtectInstaller_11.0.sh` or `ProtectInstaller64_11.0.sh`) to a local directory on the detection server.

`ProtectInstaller_11.0.sh` and `ProtectInstaller64_11.0.sh` 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.

- 4 Change to the directory where you copied the `ProtectInstaller_11.0.sh` or `ProtectInstaller64_11.0.sh` file and run the installer, by entering:

```
./ProtectInstaller_11.0.sh
```

If your system does not support a graphical user interface, run the installer by entering `-c` after the file name. For example:

```
./ProtectInstaller_11.0.sh -c
```

The installer files unpack, and a welcome notice appears.

- 5 Click **Next**.

The **License Agreement** panel appears.

- 6 After reviewing the license agreement, select **I accept the agreement**, and click **Next**.

The **Select Components** panel appears.

- 7 In the **Select Components** panel, select **Detection** and click **Next**.

- 8 In the **Hosted Network Prevent** panel, select the **Hosted Network Prevent** option only if you are installing a Network Prevent (Email) or Network Prevent (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 13.

See [“Using sslkeytool to generate new Enforce and detection server certificates”](#) on page 39.

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

`/opt/Vontu`

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.

- 10 In the **Select Directory for Symlinks** panel, select one of the options and then click **Next**.

- If you want to use symbolic links with Symantec Data Loss Prevention, enter a Destination directory. The default is `/usr/local/bin`. However, you can click **Browse** to navigate to a different location. Symbolic links let you run a program without having to specify the entire path.
- Otherwise, select **Don't create symlinks**.

- 11 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.

- 12 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.

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

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.
- 14 Restart any antivirus, pop-up blocker, or other protection software that you disabled before starting the Symantec Data Loss Prevention installation process.
- 15 Verify the detection server installation.
See [“Verifying a detection server installation”](#) on page 51.
- 16 Use the Enforce Server administration console to register the detection server with the Enforce Server.

During the server registration process, you select the type of detection server.
See [“Registering a detection server”](#) on page 51.

Verifying a detection server installation

After installing a detection server, verify that it is correctly installed before registering it.

See [“Installing a detection server”](#) on page 48.

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
`/opt/Vontu/.install4j/installation.log`
 - Symantec Data Loss Prevention operational logs are in `/var/log/Vontu`

Registering a detection server

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

See [“Verifying a detection server installation”](#) on page 51.

Once 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 (Email) Server select **Network Prevent for E-mail**.
- For Network Prevent (Web) Server select **Network Prevent for Web**.
- For Endpoint Server select **Endpoint**.
- For Classification Server select **Classification**.

See “[About detection servers](#)” on page 45.

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 81.
- 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.

Performing a single-tier installation

This chapter includes the following topics:

- [Installing a single-tier server](#)
- [Verifying a single-tier installation](#)

Installing a single-tier server

Before performing a single-tier installation:

- Complete the preinstallation steps.
See [“Symantec Data Loss Prevention preinstallation steps”](#) on page 21.
- Verify that the system is ready for installation.
See [“Verifying that servers are ready for Symantec Data Loss Prevention installation”](#) on page 23.
- 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*.

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_11.0.sh` or `ProtectInstaller64_11.0.sh` file, license file, and solution pack file have been copied into the `/opt/temp` directory on the Enforce Server.

To install the single-tier server

- 1 Log on as root to the computer that is intended for the Symantec Data Loss Prevention single-tier installation.
- 2 Copy the Symantec Data Loss Prevention installer (`ProtectInstaller_11.0.sh` or `ProtectInstaller64_11.0.sh`) from `DLPDownloadHome` to a local directory on the Enforce Server computer.
- 3 Go to the directory where you copied the `ProtectInstaller_11.0.sh` file and run the installer, by entering:

```
./ProtectInstaller_11.0.sh
```

If your system does not support a graphical user interface, run the installer by entering `-c` after the file name. For example:

```
./ProtectInstaller_11.0.sh -c
```

- 4 The installer files unpack, and a welcome notice appears. Click **Next**.
The **License Agreement** panel appears.
- 5 In the **License Agreement** panel, select **I accept the agreement**, and click **Next**.
The **Select Components** panel appears.
- 6 In the **Select Components** panel, select the **Single Tier** installation option, and click **Next**.
The **License File** panel appears.
- 7 Browse to the directory containing your license file. Select the license file, and click **Next**.
License files have names in the format `name.slf`.
The **Select Destination Directory** panel appears.

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

`/opt/Vontu`

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

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

- 9 In the **Select Directory for Symlinks** panel, select one of the following options and then click **Next**:

- If you want to use symbolic links with Symantec Data Loss Prevention, enter a Destination directory. The default is `/usr/local/bin`. However, you can click **Browse** to navigate to a different location. Symbolic links let you run a program without having to specify the entire path.
- Otherwise, select **Don't create symlinks**.

- 10 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.

The **Administrator Password** panel appears.

- 11 In the **Administrator Password** panel, enter the Administrator user account password to access the Enforce Server administration console, and confirm the password. Then click **Next**.

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.

- 12 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**.

- 13** 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**.

- 14** In the **Oracle Paths** panel, specify the location of the Oracle Base and Oracle Home directories and then click **Next**.

The following locations are the defaults:

- Oracle Base: `/opt/oracle`
- Oracle Home Directory: `/opt/oracle/product/11.2.0/db_1`

If your Oracle directories are not in the default locations, click **Browse** to locate them.

- 15** 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.

The **Final Confirmation** panel appears.

- 16** In the **Final Confirmation** panel, select one of the following options:

- For a new Symantec Data Loss Prevention installation, select the **Initialize Enforce Data** option.

You can also select 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.
- You want to add an instance of Enforce to the network and you want it to report to the existing database.

Clearing the **Initialize Enforce Data** check box skips the database initialization process.

- 17 Click **Next** to start the installation process.

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.

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

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

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

See [“Verifying a single-tier installation”](#) on page 59.

- 20 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 33.

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

See [“Registering a detection server”](#) on page 51.

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.

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
`/opt/Vontu/.install4j/installation.log`
 - Symantec Data Loss Prevention operational logs are in `/var/log/Vontu`
 - Oracle logs can be found in `/opt/oracle/product/10.2.0/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 33.

After importing a solution pack, register a detection server.

See [“Registering a detection server”](#) on page 51.

Implementing Symantec DLP Agent management

This chapter includes the following topics:

- [About implementing Symantec DLP Agent endpoint management](#)
- [Installing the Data Loss Prevention Integration Component](#)
- [Configuring the Symantec Management Platform for use with the Integration Component](#)

About implementing Symantec DLP Agent endpoint management

A Symantec Data Loss Prevention installation that includes Endpoint Discover or Endpoint Prevent requires the Symantec Management Platform for endpoint management. Symantec DLP Agent management simplifies the administration of the Endpoint Discover and Endpoint Prevent products on the endpoints.

See [“Installing the Data Loss Prevention Integration Component”](#) on page 62.

See [“Configuring the Symantec Management Platform for use with the Integration Component”](#) on page 64.

For additional information, refer to the following documentation:

- "Installing the Symantec Management Platform Products," article 45732 in the Altiris Knowledgebase at <https://kb.altiris.com>. 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.
- The *Symantec Data Loss Prevention Administration Guide* contains information about managing your Symantec DLP Agent installations, upgrades, deployments, and troubleshooting.

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," article 45732 in the Altiris Knowledgebase at <https://kb.altiris.com>. 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 7-1 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. | <p>See the <i>Symantec Data Loss Prevention System Requirements and Compatibility Guide</i>.</p> <p>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.</p> <p>For more information, see "Installing the Symantec Management Platform Products," article 45732 in the Altiris Knowledgebase at https://kb.altiris.com.</p> |
| Step 2 | Install the Symantec Installation Manager. | <p>The Symantec Installation Manager manages the installation of the Symantec Management Platform and solutions.</p> <p>See the <i>Symantec Management Platform Installation Guide</i> for instructions to install the software.</p> <p>Symantec Data Loss Prevention provides the Symantec Installation Manager installer application in the ZIP file:</p> <p><code>DLPDownloadHome/DLP/Symantec_DLP_11.0_Lin/11.0_Lin/Endpoint/SymantecDLPWinAgentMgmt_11.0.zip</code></p> <p>Note: The Symantec Management Platform can only be installed on Windows systems. You cannot install Symantec Management Platform on a Linux system.</p> |
| Step 3 | Install the Data Loss Prevention Integration Component. | <p>Use the Symantec Installation Manager to install the Data Loss Prevention Integration Component.</p> <p>For more information, see "Installing the Symantec Management Platform Products," article 45732 in the Altiris Knowledgebase at https://kb.altiris.com.</p> <p>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.</p> |
| Step 4 | Configure the Symantec Management Platform. | <p>Define roles and permissions for Symantec DLP Agent management.</p> <p>See "Configuring the Symantec Management Platform for use with the Integration Component" on page 64.</p> |

Table 7-1

Implementation of Symantec DLP Agent Endpoint management
(continued)

| Step | Action | Description |
|--------|---|---|
| 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 <i>Symantec Data Loss Prevention Administration Guide</i> . |
| Step 7 | Deploy the Altiris Agent and the Symantec DLP Agent to the endpoints, and verify the deployment. | See the <i>Symantec Data Loss Prevention Administration Guide</i> . |

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 62.

Post-installation tasks

This chapter includes the following topics:

- [About post-installation tasks](#)
- [About post-installation security configuration](#)
- [About system events and syslog servers](#)
- [Performing initial setup tasks on the Enforce Server](#)

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 67.

See [“About system events and syslog servers”](#) on page 79.

See [“Performing initial setup tasks on the Enforce Server”](#) on page 79.

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 69.

See [“About Symantec DLP Agent security”](#) on page 72.

See [“Symantec Data Loss Prevention directory and file exclusion from antivirus scans”](#) on page 77.

See [“Corporate firewall configuration”](#) on page 78.

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 provides a Web interface—the Enforce Server administration console—for reporting and administration. 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 69.
See [“Generating a unique browser certificate”](#) on page 70.
- 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 37.

See [“Using sslkeytool to generate new Enforce and detection server certificates”](#) on page 39.

See [“About post-installation tasks”](#) on page 67.

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 70.

See [“About server security and SSL/TLS certificates”](#) on page 68.

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 81.

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:

If the `/opt/Vontu/jre/bin` directory is not on your path, use `./keytool` to run it from the current directory.

```
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 `/opt/Vontu/Protect/tomcat/conf` directory.
- 7 Restart the Vontu services on the Enforce Server.
See [“About Enforce Server services”](#) on page 81.

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 68.

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 74.

See [“Running the endpointkeytool utility”](#) on page 74.

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 74.

See [“Running the endpointkeytool utility”](#) on page 74.

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 74.

See [“About Symantec DLP Agent security”](#) on page 72.

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 |
|---|--|
| <code>-keysize=<128/192/256></code> | Specifies the bit-size of the generated key file. |
| <code>-pwd=tools_password</code> | Specifies the password to access the endpoint tools. By default, the password is <i>VontuStop</i> . You must specify a password. |
| <code>[-dir=directory]</code> | The optional <code>-dir</code> 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 72.
See [“About endpointkeytool utility”](#) on page 74.
See [“About the authentication key”](#) on page 73.

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 77.

See [“Oracle directory and file exclusion from antivirus scans”](#) on page 78.

See [“About post-installation tasks”](#) on page 67.

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
- /var/log/Vontu(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
- /var/log/Vontu (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 76.

See [“Oracle directory and file exclusion from antivirus scans”](#) on page 78.

See [“About post-installation tasks”](#) on page 67.

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:

- `/opt/oracle/oradata/protect`
- `/opt/oracle/product/11.2.0/db_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 76.

See [“Symantec Data Loss Prevention directory and file exclusion from antivirus scans”](#) on page 77.

See [“About post-installation tasks”](#) on page 67.

Corporate firewall configuration

This section assumes that the Enforce Server is installed inside your corporate LAN behind a firewall, and that your detection servers (for example, your Network Monitor Servers) are installed in the DMZ.

If this is the case, your corporate firewall settings needs 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 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.

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.

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

- 4 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.

- 5 Configure any detection servers that you registered with the Enforce Server.
- 6 If you installed Network Discover, set up Discover targets.
- 7 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.

Starting and stopping Symantec Data Loss Prevention services

This chapter includes the following topics:

- [About Enforce Server services](#)
- [Starting and stopping services on Linux](#)

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 9-1 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 9-1 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. |

Starting and stopping services on Linux

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

- See [“Starting an Enforce Server on Linux”](#) on page 82.
- See [“Stopping an Enforce Server on Linux”](#) on page 83.
- See [“Starting a detection server on Linux”](#) on page 83.
- See [“Stopping a detection server on Linux”](#) on page 83.
- See [“Starting services on single-tier Linux installations”](#) on page 84.
- See [“Stopping services on single-tier Linux installations”](#) on page 84.

Starting an Enforce Server on Linux

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

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

- 1 On the computer that hosts the Enforce Server, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

- 4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

See [“Stopping an Enforce Server on Linux”](#) on page 83.

Stopping an Enforce Server on Linux

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

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

- 1 On the computer that hosts the database, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop  
./VontuIncidentPersister.sh stop  
./VontuManager.sh stop  
./VontuMonitorController.sh stop  
./VontuNotifier.sh stop
```

See [“Starting an Enforce Server on Linux”](#) on page 82.

Starting a detection server on Linux

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

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

- 1 On the computer that hosts the Enforce Server, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 To start the Symantec Data Loss Prevention services, enter:

```
./VontuMonitor.sh start  
./VontuUpdate.sh start
```

See [“Stopping a detection server on Linux”](#) on page 83.

Stopping a detection server on Linux

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

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

- 1 On the computer that hosts the database, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop  
./VontuMonitor.sh stop
```

See [“Starting a detection server on Linux”](#) on page 83.

Starting services on single-tier Linux installations

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

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

- 1 On the computer that hosts the Symantec Data Loss Prevention server applications, log on as root.
- 2 Change directory to `/opt/Vontu/Protect/bin`.
- 3 Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

- 4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start  
./VontuMonitor.sh start  
./VontuIncidentPersister.sh start  
./VontuUpdate.sh start  
./VontuMonitorController.sh start
```

See [“Stopping services on single-tier Linux installations”](#) on page 84.

Stopping services on single-tier Linux installations

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

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

- 1** On the computer that hosts the Symantec Data Loss Prevention servers, log on as root.
- 2** Change directory to `/opt/Vontu/Protect/bin`.
- 3** To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop  
./VontuIncidentPersister.sh stop  
./VontuManager.sh stop  
./VontuMonitor.sh stop  
./VontuMonitorController.sh stop  
./VontuNotifier.sh stop
```

See [“Starting services on single-tier Linux installations”](#) on page 84.

Uninstalling Symantec Data Loss Prevention

This chapter includes the following topics:

- [Uninstalling a server from a Linux system](#)

Uninstalling a server from a Linux system

You can uninstall Symantec Data Loss Prevention from a Linux-based Enforce Server or detection server. The uninstall file is located in the `/opt/Vontu` directory.

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 Linux server

- 1 Log on as root and enter the following at a command prompt:

```
# /opt/Vontu/uninstall
```

The uninstallation program begins and the Uninstall screen appears.

If your system does not support a graphical user interface, run the uninstallation program by entering `-c` after the file name:

```
# /opt/Vontu/uninstall -c
```

- 2 Click **Next** to uninstall.

- 3** When the uninstall process is finished the **Uninstall Complete** panel appears.
- 4** To complete the uninstall process, click **Done**.

Installing Symantec Data Loss Prevention with the FIPS encryption option

This appendix includes the following topics:

- [About FIPS encryption](#)
- [Installing Symantec Data Loss Prevention with FIPS encryption enabled](#)
- [Configuring Internet Explorer when using FIPS](#)

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 90.

Note: All of your Symantec Data Loss Prevention servers and agents must run either one or the other 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 90.

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 89.

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_11.0.sh -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 25.

See [“Installing a detection server”](#) on page 48.

See [“Installing a single-tier server”](#) on page 55.

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 90.

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

Symbols

64-bit installer 22

A

Administrator Account panel 57
Administrator Password panel 28
agent management 61
 implementation steps 64
AL32UTF8 character set 29
antivirus software
 scan exclusions, DLP 77
 scan exclusions, Oracle 78
authentication key 73

B

browser certificates 69
 creating 70

C

certificates
 browser 69
 browser, creating 70
 self-signed, creating 70
 server, generating 39
 SSL/TLS 68
 sslkeytool 37, 39
classification server 47

D

Data Loss Prevention Integration Component 62
 Symantec Management Platform 64
database. *See* Oracle database
detection server installation 48
 permissions 48
 preparations 48
 ProtectInstaller64_11.0.sh 49
 ProtectInstaller_11.0.sh 49
 registering 51
 remote indexers 47
 Select Components panel 49

detection server installation (*continued*)
 Select Destination Directory panel 50
 Select Directory for Symlinks panel 50
 System Account panel 50
 Transport Configuration panel 50
 types of 45
 verifying 51
DLPDownloadHome directory 14

E

Endace cards 14
 dagsnap command 24
 SPAN tap 23
endpoint tools
 endpointkeytool utility 74
endpointkeytool utility 74
Enforce server installation 25
 Administrator Password panel 28
 Final Confirmation panel 29
 initial setup tasks 79
 Initialize Enforce Data 29
 installation steps 26
 Oracle Database Server Information panel 28
 Oracle Database User Configuration panel 29
 Oracle Listener Port panel 29
 Select Components panel 26
 Symantec Management Console panel 28
 System Account panel 28
 verifying 30

F

Final Confirmation panel 29, 58
FIPS encryption 26, 89–90
 Internet Explorer, configuration 90
 VJCEProviderType=FIPS parameter 90
firewall configuration 78

I

initial setup tasks 79
Initialize Enforce Data 29

Initialize Enforce Data panel 58
 installation 11
 See also detection server installation
 See also Enforce server installation
 See also single-tier installation
 See also three-tier installation
 See also two-tier installation
 Data Loss Prevention Integration Component 62
 FIPS encryption 89–90
 logs 31, 60
 materials, required 14
 presintallation steps 21
 servers, verifying before installation 23
 system requirements 13
 uninstalling 87
 VJCEProviderType=FIPS parameter 90

K

keystore 72
 keytool command 70
 options 71

L

license files 14
 logs 31, 60

N

NIC cards 14, 23

O

Oracle database
 AL32UTF8 character set 29
 OracleOraDb10g_home1TNSListener service 30
 OracleServicePROTECT service 30
 required character set 29
 software 14
 Oracle Database Server Information panel 28, 58
 Oracle Database User Configuration panel 29, 58
 Oracle Listener Port panel 29
 Oracle Paths panel 58
 OracleOraDb10g_home1TNSListener service 30
 OracleServicePROTECT service 30

P

ports
 10026 (telnet) 24
 1521 (Oracle Listener Port) 58

ports *(continued)*

 25 (SMTP) 24
 3389 (RDP) 24
 3389 (Windows Remote Desktop Client) 79
 443 (SSL) 24
 8100 (Enforce - detection) 50, 52, 57
 Enforce - detection connection range 50, 52
 Oracle Listener 29, 58
 post-installation tasks 67
 initial system setup 79
 security configuration 67
 syslog servers 79
 preinstallation steps 21
 ProtectInstaller64_11.0.sh 22, 26
 ProtectInstaller_11.0.sh 22, 26, 49, 56

R

registering a detection server 51
 requirements 13
 materials 14

S

security configuration 67
 antivirus software 76
 browser certificates 69
 browser certificates, creating 70
 certificate, self-signed 70
 firewall configuration 78
 self-signed certificate 70
 SSL/TLS certificates 68
 virus scan exclusions 77
 virus scan exclusions, Oracle 78
 Select Components panel 26, 49, 56
 Select Destination Directory panel 50, 56
 Select Directory for Symlinks panel 50, 57
 single-tier installation 11, 55
 Administrator Account panel 57
 Final Confirmation panel 58
 high-level steps 20
 Initialize Enforce Data panel 58
 Oracle Database Server Information panel 58
 Oracle Database User Configuration 58
 Oracle Paths panel 58
 ProtectInstaller_11.0.sh 56
 Select Components panel 56
 Select Destination Directory panel 56
 Select Directory for Symlinks panel 57
 System Account panel 57

- single-tier installation *(continued)*
 - Transport Configuration panel 57
 - verifying 59
- 64-bit installer 22
- solution packs 33
 - file names 22
 - importing 34
 - list of 34
 - SolutionPackInstaller 36
- SolutionPackInstaller 36
- SPAN port/tap 23
- SSL/TLS certificates 68
- sslkeytool 37
 - generating server certificates 39
 - options 38
- Symantec DLP Agent
 - authentication key 73
 - security 72
- Symantec Management Console panel 28
- Symantec Management Platform
 - Data Loss Prevention Integration Component 64
 - security roles and permissions 64
- syslog servers 79
- System Account panel 28, 50, 57
- system events 79
- system requirements 13

T

- three-tier installation 11
 - high-level steps 15
- tiers, installation 11
- Transport Configuration panel 50, 57
- two-tier installation 11
 - high-level steps 18

U

- uninstalling 87

V

- verification
 - detection server installation 51
 - Enforce Server installation 30
 - servers ready for installation 23
 - single-tier installation 59
- VJCEProviderType=FIPS parameter 90
- Vontu services
 - starting 82–84
 - stopping 82–84

W

- Wireshark 14