Symantec™ Data Loss Prevention Upgrade Guide for Linux

Version 11.0

Symantec

Symantec Data Loss Prevention Upgrade Guide for Linux

Documentation version: 11.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

What's new and what's changed in Symantec Data Loss Prevention

This chapter includes the following topics:

Symantec Data Loss Prevention 11.0 features and changes

The following sections describe the new features and changes that were introduced in Symantec Data Loss Prevention version 11.0:

- See "New installation and upgrade features in version 11.0" on page 12.
- See "New Endpoint features in version 11.0" on page 13.
- See "New Network Discover and Network Protect features in version 11.0" on page 15.
- See "New Network Monitor and Network Prevent features in version 11.0" on page 17.
- See "New detection features in version 11.0" on page 17.
- See "New report features in version 11.0" on page 18.
- See "New language support in version 11.0" on page 18.
- See "New Data Classification features in version 11.0" on page 19.

- See "New product documentation features in version 11.0" on page 20.

New installation and upgrade features in version 11.0

Symantec Data Loss Prevention 11.0 is a major upgrade to the Symantec Data Loss Prevention product. Version 11.0 offers several new options when you install a new version of the software or upgrade from a previous version:

- 64-bit operating system support
  Symantec Data Loss Prevention servers run in 64-bit mode on compatible 64-bit operating systems. Symantec Data Loss Prevention servers are supported on the 64-bit versions of Windows Server 2008 R2 or later and Red Hat Enterprise Linux 5 Update 2 or later. In multi-tier Symantec Data Loss Prevention deployments, the Enforce Server and detection servers can be deployed on any combination of 32-bit and 64-bit server software.
  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. See the *Symantec Data Loss Prevention Installation Guide* for your platform.
- Oracle 11g support
  Symantec Data Loss Prevention supports Oracle 11g R2 11.2.0.1.0 (32-bit or 64-bit) or Oracle 10g 10.2.0.4.3 (32-bit) for storing the Enforce database. All new installations should install and use Oracle 11g to ensure continued support for security and stability patches. Existing Oracle 10g customers should upgrade to Oracle 11g as necessary to receive continued security updates. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.
- Network Prevent installation to a hosted environment
  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). 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.
  If you choose to install a detection server to 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 with hosted detection servers.
  See the *Symantec Data Loss Prevention Installation Guide* for your platform.

- Flexible upgrade window for detection servers
  Symantec Data Loss Prevention version 11 enables you to upgrade version 10.x detection servers in stages, while still using non-upgraded detection servers to monitor and prevent confidential data loss. To upgrade to version 11, you begin by upgrading the Enforce Server. The upgraded Enforce Server can communicate with version 10.x detection servers for the purpose of recording new incidents and preventing confidential data loss. You should then upgrade the remaining detection servers as soon as possible to reduce the risk of those servers becoming temporarily unavailable. This can happen if those servers stop or restart after the Enforce Server is upgraded.
  See "Upgrade requirements and restrictions" on page 39.

See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for more information about hardware, operating system, and third-party software support in version 11.0.

New Endpoint features in version 11.0

For Endpoint, the following new features are available in version 11.0:

- Agent configurations
  You can create different configuration modules for groups of Endpoint Servers. Agent configurations replace most of the Endpoint Server configuration functionality of previous releases.
  You can assign agent configurations to Endpoint Servers through the Enforce Server administration console or to individual Symantec DLP Agent through the Symantec Management Console (SMC). However, you can only create agent configurations through the Enforce Server administration console.
- Endpoint Discover Quarantine response rule
  The Endpoint Discover Quarantine response rule lets you move confidential files to a secure location. Quarantine response rules are only applicable on Endpoint Discover. The secure location can either be the local drive, or it can be a confidential folder on a remote file share.
- Application monitoring
  The application monitoring feature lets you specify third-party applications for data loss prevention monitoring.
- Endpoint FlexResponse
  Endpoint FlexResponse lets you develop your own response plug-ins and use them to remediate incidents. Symantec Data Loss Prevention supports Python-scripted plug-in modules that can be embedded as Endpoint response rules.
- Rule Results Caching (RRC)

RRC is a way for the Symantec DLP Agent to save the results of previously scanned files. If a file does not violate a policy, the results of the scan are saved. Then, if the file is not modified, the file passes through the detection server without being scanned again. Using the results of previous scanning improves performance and saves time because the agent does not need to re-scan files that are already known to be safe.

- Improved agent health statuses
  Agent health statuses now include more in-depth statuses such as "Disabled," "Disconnected," and "Under Investigation." These health statuses let you have a deeper understanding of how your Symantec DLP Agents perform. The new agent health statuses also reflect agent troubleshooting tasks. Additionally, information has been added to the agent status to reflect the last connection time of the agent. When the agent connects to the Endpoint Server, the time of the connection is recorded. The most recent connection time is displayed. You can use this connection time marker to see if new policies have been distributed to your agents.
- Agent troubleshooting tasks
  Agent troubleshooting tasks let you take direct action on agents that may or may not be performing properly. These tasks include Changing the Endpoint Server, Pull Logs, Disable Agent, and Set Under Investigation, among others. The agent troubleshooting tasks are applicable to any agent that is registered with the Enforce Server administration console.
- Symantec Management Platform version 7.1 support
  The Symantec Management Console (SMC) now supports Symantec Management Platform (SMP) version 7.1. Previously, the only supported version of SMP was 7.0.
- Improved hard drive monitoring
  You can now perform Endpoint Prevent on data transferring from a network share to your local drive.
- Removable media metadata policy condition
  Policy authors can detect one or more specific endpoint devices or an entire class of device, such as a USB flash drive from a specific hardware vendor.
- Firefox version 3.7 support
  Firefox version 3.7 is now supported.
- 64-bit Microsoft Outlook 2010 support
  Microsoft Outlook 2010 64-bit is now supported.

New Network Discover and Network Protect features in version 11.0

For Network Discover and Network Protect, the following new features are available in version 11.0:

- Folder risk reporting
  The new folder risk report ranks folders based on number of files with policy violations, severity weightings, folder exposure, and actual user accesses on sensitive data.
  This report provides a mechanism to focus on the folder assets with the largest volume of data and highest risk of data exposure and helps Symantec Data Loss Prevention remediators drive down risk in the fastest possible manner.
  This new report has the following information about the risk of the folders in the list:
  - List of folders and calculated risk values
  - Link to an incident summary report
  - The top five data owners of sensitive files
  - Monthly access trends for the last 12 months
  - File activity of the groups that are listed in the folder access control list (ACL)
- Data-owner remediation reports
  Data-owner remediation reports provide a scalable method of remediating large numbers of incidents.
  You can aggregate incidents into a single incident report for each data owner on an ad hoc or scheduled basis and then email the remediation reports (as a CSV or HTML attachment) to the respective custodians or data owners.
  Two new fields are in the incidents:
  - Data Owner Name
  - Data Owner Email Address
- Enhanced SharePoint scanning
  A new Network Discover target for SharePoint 2007 and SharePoint 2010 enables integrated configuration and control of SharePoint scans.
  The following features are included in the enhanced SharePoint scan target:
  - Supports SharePoint 2010.
  - Simplifies the configuration for scanning SharePoint sites. Provides the ability to start, stop, and pause SharePoint scans manually or according to a preconfigured schedule.

- Easily filter on sites for targeting and provides throttling to control scan overhead.
- Provides for secure data transfer when the SharePoint sites are configured to use SSL. Also, allows optional secure setup with Kerberos authentication.
- Integrates with the Enforce Credential Management function to enable the use of granular user privileges for scanning sites.
- Reports SharePoint ACLs in Discover incident snapshots, and allows report filtering on SharePoint permissions and users or groups.
- Scans all content under SharePoint document libraries, Tasks, Discussion Items, Wiki pages, blogs, Calendar entries, Tasks, Contact lists, Announcements, Attachments, Lists, and Custom Lists.

The current Sharepoint scanners are also retained in this release, so that customers with existing scanner targets (SharePoint 2003 and 2007) can continue to use them. The SharePoint scanners are deprecated in this release.

- Enhanced Exchange scanning

  A new Network Discover target for Exchange 2003 and 2007 servers enables integrated configuration and control of the scans of Exchange servers.
  The following features are included in the enhanced Exchange scan target:

  - Simplifies the configuration for scanning Exchange servers. Provides the ability to start, stop, and pause Exchange scans manually or according to a preconfigured schedule.
  - Easily filter on sites for targeting and provides throttling to control scan overhead.
  - Integrates with the Enforce Credential Management function to enable the use of granular user privileges for scanning sites.

  The current Exchange scanner is also retained in this release, so that customers with existing scanner targets can continue to use them. The Exchange scanner is deprecated in this release.

- Incremental scanning

  With Incremental scanning on file shares, you only scan those files that have not been scanned before and those files that have been modified since the last scan. Incremental scanning can provide a significant improvement in the time it takes to complete subsequent scans. Incremental scanning is also invaluable when items are missed due to files or shares being inaccessible, or if your scan fails before it is finished—you do not need to do another full scan of all content to cover the missed items.

New Network Monitor and Network Prevent features in version 11.0

For Network Prevent and Network Monitor, the following new features are available in version 11.0:

- Hosted deployment for Network Prevent
  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). The Enforce Server and all other detection servers must reside in the corporate network and communicate over a LAN.
  If you choose to install a detection server to 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 with hosted detection servers.
  See the *Symantec Data Loss Prevention Installation Guide* for your platform.
- High-speed packet capture for Network Monitor
  Network Monitor provides improved capture performance on Windows platforms. Windows Server 2003 SP2 (32-bit) and Windows Server 2008 R2 (32-bit or 64-bit) users can now monitor high-speed, gigabit networks without deploying and maintaining specialized packet capture cards or measurement devices. See the *Symantec Data Loss Prevention Network Performance and Sizing Guide* for more information.

New detection features in version 11.0

Symantec Data Loss Prevention version 11.0 offers several new policy detection features.

These new features include:

- Custom Data Identifiers
  The patterns and validators for all system-defined Data Identifiers are exposed to policy authors for customization and tuning. Administrators can also define entirely new Data Identifiers using their own patterns and validators.
- Server-side group-based policies
  Policy authors can detect the exact identities of data users based on their group affiliation in a directory server. Policy authors can detect sender and recipient identities and endpoint computer users by synchronizing with Microsoft Active Directory.

- Keyword proximity matching and wildcard character
  Policy authors can define pairs of keyword groups and specify proximity between them for more accurate ways of describing data. The wildcard character allows for partial suffix matching.
- Data owner exception
  Policy authors can exclude data owners from Exact Data Matching detection based on email or domain address when data owners send or receive their own confidential data.
- Authorized endpoint devices
  Policy authors can configure one or more classes of endpoint devices, such as encrypted USB drives, for allowable use scenarios.
- Detection for email Subject
  Policy authors now have the option to target a detection rule to the Subject of an email message.
- Response rule ordering
  Response rule authors can order the execution among response rules of similar type.
- Content Extraction API
  Developers can perform file type identification, text filtering, file extraction, or advanced processing like decryption or OCR.

New report features in version 11.0

The following new reporting features are available in version 11.0:

- Reporting API updates
  The incident details schema used in the Reporting Web Services API has been updated to support additional incident detail fields added for Symantec Data Loss Prevention features.
  See the *Symantec Data Loss Prevention Reporting API Developers Guide* for more information.
- Folder risk reporting
  See "New Network Discover and Network Protect features in version 11.0" on page 15.

New language support in version 11.0

The Enforce Server administration console user interface is now available in Spanish, Brazilian Portuguese, and Traditional Chinese. The DLP IC component user interface is now available in Spanish and Brazilian Portuguese.

For detailed information about Symantec Data Loss Prevention international feature support, including translated versions and languages that are supported for detection, see the *Symantec Data Loss Prevention Administration Guide*.

New Data Classification features in version 11.0

Symantec Data Loss Prevention v11.0 includes a new type of detection server, and new detection and policy features, that enable Symantec Enterprise Vault for Microsoft Exchange users to classify messages for archiving and compliance review. The Classification Server enables a Symantec Enterprise Vault for Microsoft Exchange filter to post messages to Symantec Data Loss Prevention for the purpose of classifying the messages. Customers can use the full policy authoring functionality of Symantec Data Loss Prevention, along with a new MAPI detection rule, to classify messages. Classification policies determine whether a message should be archived or deleted, and whether to flag the message for compliance review or E-Discovery searches. The policies also determine the classification tag and retention category to assign to the message. The Classification Server returns the result tags back to the Enterprise Vault for Microsoft Exchange filter. Enterprise Vault for Microsoft Exchange uses the tags to perform archiving, delete messages, and assign compliance reviews for the message. The Discovery Accelerator and Compliance Accelerator products can also leverage classification tags to filter messages during searches or audits.

Note: The Classification Server is used only with the Symantec Data Classification for Enterprise Vault solution, which is licensed separately from Symantec Data Loss Prevention. You must configure the Enterprise Vault Exchange Agent filter and Classification Server to communicate with one another. See the *Symantec Enterprise Vault Data Classification Services Implementation Guide* for more information.

The Classification Server is installed and registered in the same way as other Symantec Data Loss Prevention detection servers. See the *Symantec Data Loss Prevention Installation Guide* for your platform for more information.

Classification policies are configured using the same Enforce Server administration console pages that you use to configure Symantec Data Loss Prevention policies. However, certain detection rules and response actions are available only if you have licensed a Classification Server. See the *Symantec Enterprise Vault Data Classification Services Implementation Guide* for more information about policy configuration features that are available with Classification policies.

New product documentation features in version 11.0

For product documentation, the following new features are available in version 11.0:

- The *Symantec Data Loss Prevention Administration Guide* and online Help were revised and reorganized to divide topics into more meaningful parts.
- Agent upgrade instructions were moved from the *Symantec Data Loss Prevention Administration Guide* to the *Symantec Data Loss Prevention Upgrade Guide* to provide easier access to these topics during an upgrade.
- The *Symantec Data Loss Prevention Custom File Type Detection Guide* was revised and renamed to the *Symantec Data Loss Prevention Detection Customization Guide*.

Symantec Data Loss Prevention 10.x features and changes

The following sections describe the new features and changes that were introduced in Symantec Data Loss Prevention versions 10.0 and 10.5:

- See "New Enforce features in version 10.x" on page 20.
- See "New detection features in version 10.x" on page 26.
- See "New Endpoint features in version 10.x" on page 21.
- See "New Network Discover and Network Protect features in version 10.x" on page 24.
- See "New Network Monitor and Network Prevent features in version 10.x" on page 25.
- See "New report features in version 10.x" on page 28.
- See "New international features in version 10.x" on page 29.

New features that were specific to Symantec Data Loss Prevention version 10.5 are labeled "(New in v10.5)."

New Enforce features in version 10.x

For Enforce, the following new features were added in version 10.x:

- New management user interface with configurable incident snapshot
  The UI of the Enforce Server administration console were completely redesigned. Incident snapshot information were arranged according to user role and requirements, enabling more effective incident remediation. The

navigation panel on the left-hand side of the console was replaced with options and menu items, located above dashboard pages. Some pages were streamlined to include tabs for accessing parts of the console interface.
Navigation details for all tasks have were revised in the online Help and in the *Symantec Data Loss Prevention Administration Guide*.

- Centralized log collection and configuration
  The Enforce Server administration console added a feature to collect log files from any or all Symantec Data Loss Prevention servers. You can also change the logging configuration of individual servers directly from the Enforce Server administration console. To change the logging configuration, you use either custom log configuration files or predefined log settings. This new Enforce Server functionality replaced the command-line Log Collection Utility (LCU).
  See the online Help for more information about the **Logs** screen (**System > Logs**).
- VMware support
  For details about the virtualization support for the Enforce Server and other Symantec Data Loss Prevention components, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*. Note that virtualization support for the Enforce Server does not include the Oracle database.
- New event codes replaced Event Summary or Event Description variables

New Endpoint features in version 10.x

For Endpoint, the following new features were added in version 10.x:

- Endpoint Prevent user groups
  Endpoint user groups let you create detection rules for Endpoint Prevent based on Active Directory groups of users. When a Symantec Data Loss Prevention group is created, it can be easily reused across multiple Symantec Data Loss Prevention policies. Endpoint Prevent user groups are created in the Enforce Server using Active Directory groups only.
- Improved file filters across language and operating system settings
  The KNOWNFOLDERID file filter change added flexibility to the Symantec DLP Agent. The KNOWNFOLDERID file filter does not use hard-coded paths to relevant file folders. Instead, it sends a query to the endpoint computer to obtain the location of the folders. The Symantec DLP Agent can access relevant file folders regardless of the operating system or language settings of the endpoint computer. Different operating systems and language settings may have different locations for the relevant file folders.
  See the Symantec Data Loss Prevention online Help.

- Internationalization options for Endpoint Prevent response rules
  Response notification messages can be created in different languages with a single response rule. The locale setting of the endpoint computer operating system determines the actual notification that appears to the user.
- Additional detection support
  Endpoint Prevent added new detection support for SD and compact flash cards, Yahoo IM 9.0, AIM Pro, MSN IM 14, and Firefox v3.1.
- Endpoint Discover scanning while idle
  You can scan your endpoint computers while they are idle. Endpoint computers are considered idle when they have not used active processes for a specified amount of time. You can set the level of the scan while idle to improve the overall performance of endpoint computers in your organization. Endpoint Discover uses fewer computer resources with this feature.
  See the Symantec Data Loss Prevention online Help for Endpoint advanced settings.
- New Agent Management features
  The Symantec Management Console added two new tasks: Toggle print screen and Change Endpoint Server.
  Toggle print screen lets you enable or disable the Print Screen functionality for each endpoint computer. Change Endpoint Server lets you specify different Endpoint Servers for endpoint computers. If the agent is not able to connect to one Endpoint Server, it attempts to connect to the next Endpoint Server in the list.
  Additionally, new reports are available, including the print screen report, which displays the endpoint computers that have active print screen monitoring.
  See the Symantec Data Loss Prevention online Help for Agent Management.
- User Cancel response rule
  The User Cancel response rule lets you create a pop-up response notification for endpoint users. This notification includes an option to allow the violating data to transfer to the destination. The endpoint user makes the decision to allow the data transfer or to cancel the transfer. An incident is created whether or not the data is transferred. The User Cancel response rule is only available with Endpoint Prevent. (New in v10.5)
- Localization support for Agent Management
  The Agent Management component (DLP IC) added localization support for English, French, Japanese, and Simplified Chinese. (New in v10.5)
  See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for more information.
- Agent Management Register Agents process

Endpoint Agent Management Register Agents process lets you register any unregistered Symantec DLP Agents with the Symantec Management Platform. Use this process if you have previously installed Symantec DLP Agents on endpoint computers before you connect the Symantec Management Console to the Enforce Server. (New in v10.5)

- Windows 7.x 64-bit support
  Symantec DLP Agents support was added for computers running Microsoft Windows 7 64-bit operating systems. (New in v10.5)
- Citrix installation
  Citrix XenDesktop and Citrix XenApp provide virtual Windows desktops and Windows applications to clients of the Citrix servers. Symantec supports deploying the Symantec DLP Agent software directly on Citrix XenApp/Application servers or Citrix XenDesktop virtual machines. This deployment prevents clients from extracting confidential data from Citrix published applications or from desktops to the client computer. Symantec Data Loss Prevention provides this functionality by monitoring volumes, print and fax requests, clipboards, and network activity on the Citrix server. This monitoring process then detects when confidential data is sent to a client computer.
  Individual Citrix clients do not require a Symantec DLP Agent installation to support this functionality. Because a single Symantec DLP Agent installation monitors multiple Citrix clients, you must purchase an Endpoint Prevent license that covers all of your Citrix clients. See your Symantec sales representative for more information.
  See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for important requirements and restrictions to consider when using the Symantec DLP Agent with Citrix servers.
- Support for Lotus Notes 6.5
  Endpoint Prevent detects violations on Lotus Notes 6.5. (New in v10.5)
- Support for Firefox 3.6
  Endpoint Prevent detects violations on Mozilla Firefox v3.6. (New in v10.5)
- Changes to Agent Management installation infrastructure
  The Agent Management installation infrastructure was changed to improve performance and stability. (New in v10.5)
- Endpoint Lockdown
  Endpoint Lockdown is a process that can disable an endpoint computer's network and removable media capabilities if a violation is detected. The endpoint computer capabilities are only restored when you remediate the incident. Endpoint Lockdown combines Symantec Data Loss Prevention, Symantec Management Platform, Symantec Endpoint Protection, and Symantec

Workflow Solution products. Endpoint Lockdown is an additional feature. Contact your Symantec representative for more information. (New in v10.5)

New Network Discover and Network Protect features in version 10.x

For Network Discover and Network Protect, the following new features are available in version 10.x:

- FlexResponse, a flexible platform for incident remediation
  The FlexResponse Platform enables the creation of comprehensive custom remediation actions for the files that are discovered using Symantec Data Loss Prevention Network Discover. FlexResponse supports Symantec and third-party file security solutions including Enterprise Digital Rights Management and encryption. FlexResponse is an extension of the Network Protect product, and the Network Protect product is required for FlexResponse functionality. See the *Symantec Data Loss Prevention FlexResponse Platform Developers Guide*.
- Stored credentials
  Credential management for Network Discover targets using stored credentials. An authentication credential can be stored as a named credential in a central credential store. It can be defined once, and then referenced by any number of Network Discover targets. Storage of authentication credentials in a central store simplifies the management of user name and password changes.
- Improved management of some scanners
  Management of the Microsoft Exchange and SharePoint 2007 scanners was improved, as was scanning of file systems and Web servers.
- Enhanced incident trend and remediation reports
  The following fields in incident snapshot reports were added: **Detection date** and **Seen Before**. You can summarize the incidents that have an earlier connected incident, by the time since the incident was last seen.
  See "New report features in version 10.x" on page 28.
- Integration with Symantec Data Insight
  During incident remediation, Symantec Data Insight helps organizations solve the problem of identifying data owners and responsible parties for information due to incomplete or inaccurate metadata or tracking information. (New in v10.5)
  With Symantec Data Insight, users can monitor file access to automatically identify the data user of a file based on the access history. The usage information then automatically feeds into the incident detail of files that violate Symantec Data Loss Prevention policies. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

Symantec Data Insight is a separately licensed option, with a connection from the Enforce Server to the Symantec Data Insight Management Server.
See the *Symantec Data Loss Prevention Data Insight Implementation Guide*.

- SharePoint 2007 scanner for Network Discover now supported on Windows 2008 Servers (New in v10.5)

New Network Monitor and Network Prevent features in version 10.x

For Network Prevent and Network Monitor, the following new features were added in version 10.x:

- Hosted email integration with Network Prevent (Email) TLS support
  Network Prevent (Email) can receive TLS-encrypted email from an upstream MTA. It can also initiate a TLS session to a downstream outbound MTA or hosted email service, as requested by the upstream MTA. The TLS capability enables you to integrate Network Prevent (Email) with a hosted email service, such as the Message Labs Email Content Control Service.
  To facilitate TLS connections, Network Prevent (Email) has a dedicated keystore file at `installdir\Vontu\Protect\keystore\prevent.ks`. The Network Prevent Server (Email) keystore must contain a public key certificate for the downstream MTA or hosted email server. If an upstream MTA authenticates the Network Prevent (Email) server as part of the TLS session, that MTA keystore must also store the public key certificate for Network Prevent (Email).
  See the *MTA Integration Guide for Network Prevent (Email)* for more information about configuring TLS support.

- MX record lookups with Network Prevent (Email)
  Network Prevent (Email) can perform an MX record lookup to determine the address of a next-hop MTA or hosted email server. This lookup capability allows Network Prevent Server (Email) to use DNS load balancing and failover capabilities when it selects the next hop MTA or hosted email server. To use the MX record lookup feature, you must enable it. You must also specify a domain name to use for MX record lookups in forwarding mode.
  See the *MTA Integration Guide for Network Prevent (Email)* for information about configuring and using MX record lookups.

- ISA support with Network Prevent (Web)
  Symantec Data Loss Prevention supports integrating Microsoft Internet Security and Acceleration Server (ISA) with Network Prevent (Web). To integrate ISA, you must install and configure the Symantec Data Loss Prevention Web filter to ISA. The Web filter uses ICAP to send Web requests and responses to one or more Network Prevent (Web) servers for inspection. The Web filter then sends, blocks, or redacts requests and responses based on the detection result that is communicated from Network Prevent (Web).

The Symantec Data Loss Prevention ISA Web filter supports request monitoring for the following HTTP request types:

- GET
- PUT
- POST
- GET FTP (FTP requests that are tunneled through HTTP)

The Web filter also supports response monitoring for a variety of response MIME types.
See the *Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server* for more information.

- Squid Web Proxy support with Network Prevent (Web)
  Symantec Data Loss Prevention supports the integration of Squid version 3.0 with Network Prevent (Web) to inspect HTTP traffic. This integrated functionality blocks or modifies the traffic that violates configured policies. The Squid integration supports only forward-proxy mode deployments using ICAP request modification (REQMOD) mode.
  See the *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy* for more information.
- Revised interface for next-hop MTA configuration (New in v10.5)
  The **Configure Server** page for Network Prevent (Email) was revised to simplify the configuration of next-hop MTAs in forwarding mode. The on-screen labels were also updated to clarify the information that is required when you enable or disable MX record lookups.
  To access the configuration page in the Enforce Server administration console, select **System > Overview**. Then, click the name of a Network Prevent (Email) detection server. Click **Configure** to display the current settings.
  See the online Help or the *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email).*
- New Web site definitions for HTTP/S content removal (New in v10.5)
  The **Network Prevent: Remove HTTP/S Content** response rule action can be used with additional Web mail, blog, and social networking sites to remove protected content from Web form fields.
  See the online Help for more information.

New detection features in version 10.x

Symantec Data Loss Prevention version 10.x added several new detection features.

These new detection features are summarized as follows:

- International character normalization on the endpoint
  For reliable comparison between text, the detection engine converts (normalizes) character variants to a base type, as prescribed by the Unicode standard. In addition, the detection engine removes new lines between successive Asian characters (for example, Simplified Chinese).
- International keyword matching
  The detection engine switches between whole-word and partial word matching automatically for the content you detect. This new keyword matching functionality improves the detection matching accuracy for keyword lists with both non-Asian (English, for example) and Asian (Chinese, for example) keywords. It also improves detection of keywords or phrases that contain both Asian and non-Asian characters (¥2000, for example).
- Policy template import and export
  You can share policies across environments by using policy import and export. You can:
  - Author and test a policy in a development environment
  - Export the policy as a template
  - Import the policy to a production system for deployment

  This feature is also useful for troubleshooting, versioning, and archiving existing policies, and installing new ones. Note that policy import and export does not include document, data profiles, or response rules.
  You can export any configured policy as a template from the policy builder interface. When you export a policy, the system generates an XML file that is human readable. You can import one or more policies by placing the XML file(s) in the "templates" directory on the Enforce Server host. In the policy templates screen you see an entry for each policy you import.
- Custom file type detection
  With Symantec Data Loss Prevention you can detect over 300 file types. To detect the presence of a file type that is not currently supported, you can use the Custom File Type Signature rule. To use this rule, you implement a custom script to match the unique signature of the proprietary file type.
  Symantec Data Loss Prevention provides a simplified scripting language that you use to detect the custom file type. In addition, Symantec Data Loss Prevention provides a utility to help you determine the unique bytes of the custom file type. You can also use this utility to test and refine your script before you configure the Custom File Type Signature rule.

New report features in version 10.x

The following reporting features were added in Symantec Data Loss Prevention version 10.x:

- Reporting API for exporting incident data

  The Symantec Data Loss Prevention Reporting Web Services API allows skilled Web Services developers to create applications that pull incident data from the Enforce Server. The incident data can be integrated with other applications or systems to provide dynamic reporting. The incident data integration also supports business processes that rely on Symantec Data Loss Prevention incidents. The Reporting API interface lets you access only the incidents and incident data that you require for a particular business process.

  For example, you can use the API to correlate Symantec Data Loss Prevention incident data with network usage. Or, you can create dashboard applications that seamlessly integrate Symantec Data Loss Prevention incident data with data from other systems, such as intrusion detection systems. The combined information can provide valuable information to security experts who are tasked with analyzing the data or with remediating security incidents.

  The Symantec Data Loss Prevention Reporting API is implemented as a Web Service that resides on the Enforce Server. The Web Service conforms to the Simple Object Access Protocol (SOAP) 1.1 standard, and it advertises all available operations using a Web Services Description Language (WSDL) document. You can use the WSDL document with compatible Web Services development frameworks to generate certain client code automatically. The API includes XML schemas to help you work with the different incident types that Symantec Data Loss Prevention supports. The schemas also enable you to integrate incident data with other data or applications.

  See the *Reporting API Developers Guide* for more information.

- XML export for incident data

  Symantec Data Loss Prevention supports exporting an incident report to an XML file. The XML file format provides several benefits over comma-separated text files (CSV files). These benefits include the ability to export complex data, such as the matches that caused the incident. XML also enables you to view or transform incident data using third-party reporting tools.

  You export incident reports to XML using the Enforce Server administration console.

  Each Symantec Data Loss Prevention product or product component may generate unique XML fields to store incident data. XML schema files for exported reports are stored in the `installdir\Vontu\Protect\tomcat\webapps\ProtectManager\WEB-INF\lib\reportingapi-schema.jar` file.

See the *Reporting API Developers Guide* for a description of individual XML elements.

- Enhanced trend and remediation reports for Network Discover incidents are available due to several new incident report options on the Enforce Server.
  The following fields were added in incident snapshot reports: **Detection date** and **Seen Before**.
  The following filters were added for incident reports:
  - **Detection date**
  - **Time since first detected**
  - **Seen before**
    A Discover incident is defined as "seen before" if an earlier Discover scan created a connected incident from the same file.

    Note: This feature is not available for SQL Database incidents, where **Seen before** is always false.

  The following summaries were added to incident reports:
  - **Months Since First Detected**
  - **Quarters Since First Detected**
  - **Weeks Since First Detected**
  - **Years Since First Detected**
  - **Detection Month**
  - **Detection Quarter**
  - **Detection Week**
  - **Detection Year**

New international features in version 10.x

Symantec Data Loss Prevention added the following international features in version 10.x.

- Expanded detection language support.
  See "New detection language support in version 10.x" on page 30.
- New language pack support.
  See "New language pack support in version 10.x" on page 30.
- New product documentation features.

See "New product documentation features in version 10.x" on page 31.

New detection language support in version 10.x

Detection support in Russian, Arabic, and Hebrew was added. You can install Symantec Data Loss Prevention on localized, and Multilingual User Interface (MUI), versions of Windows for these languages. You can also define policies that accurately detect and report on violations found in content written in these languages. Language support does not, however, include a translated Symantec Data Loss Prevention administration console UI in these languages.

Symantec Data Loss Prevention can inspect content that is written in Turkish for policy violations. But, you cannot install Symantec Data Loss Prevention on a Windows operating system that is localized for the Turkish language. Nor can you choose Turkish as an alternate locale.

For detailed information about Symantec Data Loss Prevention international feature support, see the *Symantec Data Loss Prevention Administration Guide*.

New language pack support in version 10.x

Language packs support was added for the following languages in Symantec Data Loss Prevention version 10.x:

- French
- Korean (New in v10.5)
- Japanese
- Simplified Chinese

Symantec Data Loss Prevention provides a command line-based language pack utility that you use to add, change, or delete locales and language packs.

When you install a language pack, Enforce Server screens, menu items, commands, and messages appear in the selected language.

The Symantec Data Loss Prevention Help system may also be displayed in the language.

Its locale ensures that Enforce Server reports and lists can be sorted alphabetically as appropriate to the locale for that language.

Numbers and dates also appear in locale-appropriate format.

For detailed information about Symantec Data Loss Prevention international feature support, see the *Symantec Data Loss Prevention Administration Guide*.

New product documentation features in version 10.x

The following product documentation features were added in version 10.x:

- Improved and expanded online Help content.
- Enhanced online Help index for easier navigation and access.
- Greater shared content between online Help and the PDF guides, making it easier to locate information and providing a choice of formats to use.
- Product documentation was localized for French, Korean (new in v10.5), Japanese, and Simplified Chinese.
- Additional guides in PDF format were added to the product documentation suite:
  - *Symantec Data Loss Prevention Data Insight Implementation Guide.* (New in v10.5)
  - *Symantec Data Loss Prevention Custom File Type Detection Guide* (previously available in the Symantec Data Loss Prevention Knowledgebase). (New in v10.5)
- The *Symantec Data Loss Prevention Utilities Guide* is no longer produced. Its content has been added to the *Symantec Data Loss Prevention Administration Guide*. (New in v10.5)
- Streamlined content that is presented in a concise, “topic-oriented” style, with cross-references to more in-depth information.
- Indexes for most PDF documents, enabling better access to information and improving the offline reading experience.

Chapter 2

Preparing to upgrade Symantec Data Loss Prevention

This chapter includes the following topics:

About preparing to upgrade Symantec Data Loss Prevention

All Symantec Data Loss Prevention upgrades must be performed incrementally from one major release to the next. From Symantec Data Loss Prevention 10.0 or 10.5, you can upgrade directly to version 11.0. But you cannot upgrade directly from versions 9.x, 8.x, or older to version 11.0. To upgrade from versions older than 10.x, you must perform each upgrade in sequence. For example, to upgrade from 8.0 you must first upgrade to 9.0, then from 9.0 to 10.0, and then from there to 11.0.

Symantec Data Loss Prevention version 11 enables you to upgrade version 10.x detection servers in stages, while still using non-upgraded detection servers to monitor and prevent confidential data loss. To upgrade to version 11, you begin by upgrading the Enforce Server. The upgraded Enforce Server can communicate with version 10.x detection servers for the purpose of recording new incidents and preventing confidential data loss. You can schedule the remaining detection server upgrades for a time that minimizes service interruption, with certain restrictions.

See "Upgrade requirements and restrictions" on page 39.

You do not need to upgrade your Oracle database when upgrading to Symantec Data Loss Prevention 11.0. However, you do need to back up your database before any upgrade. You may choose to upgrade to Oracle 11g at a later time to ensure continued security patches. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for more information.

Symantec Data Loss Prevention upgrade phases

An upgrade is performed in the phases described as follows.

Table 2-1 Symantec Data Loss Prevention upgrade phases

Phase	Action	Description
Phase 1	Review important information about the current release before starting the upgrade, including: ■ Minimum system requirements. ■ Restrictions regarding upgrades to mixed operating systems. ■ Language pack requirements. ■ Known release issues. ■ Planning how to upgrade your system.	See the *Release Notes* to learn about any known upgrade issues or issues with the current release of Symantec Data Loss Prevention. See "About the minimum system requirements for upgrading to the current release" on page 36. See "About upgrading installations with mixed operating systems" on page 36. See "Supported upgrade backward compatibility for agents and servers" on page 37. See "About the requirement for language pack upgrades" on page 38. See "Upgrade requirements and restrictions" on page 39. See "About choosing an upgrade method" on page 40.
Phase 2	Prepare the system for upgrading. This preparation includes a backup of the Oracle database and detection server data. Without these preparations your upgrade can fail.	See "Preparing your system for the upgrade" on page 40.
Phase 3	Download and extract the version 11.0 software.	See "Downloading and extracting the upgrade software" on page 46.
Phase 4	Using the Upgrade Wizard, upgrade the Enforce Server and any detection servers running on the same operating system. If necessary, perform a local upgrade on any detection servers that were not upgraded using the Upgrade Wizard.	See "Performing an upgrade with the Upgrade Wizard" on page 49. See "Locally upgrading a detection server" on page 52.
Phase 5	Upgrade Symantec Data Loss Prevention Agents. Upgrade any scanners. If appropriate, implement Symantec DLP Agent Endpoint management. If appropriate, implement the Symantec Management Platform and DLP Integration Component.	See "Upgrading your scanners" on page 54.

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

Phase	Action	Description
Phase 6	Complete the required and optional post-upgrade tasks.	See "Performing post-upgrade tasks" on page 63.
Phase 7	Upgrade your database to Oracle 11g.	Upgrade your database to ensure continued security fixes. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.

About the minimum system requirements for upgrading to the current release

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

- Enforce Server single-, two- or three-tier installation: 50 GB (for small/medium enterprise) to 100 GB (for large/very large enterprise) of free disk space on the volume where the server is installed.
- Detection server: 300 MB of free disk space on the volume where the server is installed.

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

See "About preparing to upgrade Symantec Data Loss Prevention" on page 34.

About upgrading installations with mixed operating systems

Some Symantec Data Loss Prevention installations have servers running on both the Linux and Windows operating systems. The Upgrade Wizard can only upgrade detection servers that are running on the same operating system as the Enforce Server. Detection servers running on a different operating system have to be upgraded locally.

If your Enforce Server is on Linux and you have detection servers on Windows, download the Windows upgrade software. Then upgrade the Windows servers

using the local upgrade instructions in the *Symantec Data Loss Prevention Upgrade Guide for Windows*.

See "Locally upgrading a detection server" on page 52.

Supported upgrade backward compatibility for agents and servers

As you upgrade your Endpoint protection, you may have different components of the suite on different versions. During the upgrade process, you may have Enforce Servers on version 11.0, Endpoint Servers on version 10.x or 11.0, and agents on versions 10.x, or 11.0. The following table describes the scenarios where multi-version servers and agents are possible. The described scenarios are only possible during the upgrade process. The scenarios assume that you have already upgraded your Enforce Server to version 11.0. You cannot upgrade either your Endpoint Servers or your agents before upgrading your Enforce Server.

If your agents and Endpoint Servers are on previous versions from 11.0, do not restart the Endpoint Server. If you restart the Endpoint Server when it is not on the current version, all policy and all configuration information is lost. If all of the policy and the configuration information is lost, you must upgrade the Endpoint Server and the agents. Endpoint Servers must be upgraded to version 11.0. Agents must be upgraded to a minimum of version 10.0. When you upgrade to the current version, upgrade the agents first and then upgrade the Endpoint Server. For example, assume that you have a version 11.0 Enforce Server, and version 10.0 Endpoint Server and agents. Upgrade the agents to version 11.0 and then upgrade the Endpoint Server to version 11.0. Upgrading the agents first minimizes the possibility that your agents and servers are arranged in an unsupported configuration.

Note: New features for version 11.0 are not available on previous versions of the Endpoint Server or agents, even if your Enforce Server is currently on version 11.0.

Table 2-2 Supported backward compatibility for agent upgrades

Enforce Server version	Endpoint Server version	Symantec DLP Agent version	Results
11.0	11.0	10.x	Policy and configuration updates are sent to the Endpoint Server and the agents. Incidents are sent to the Enforce Server. New features for 11.0 are not available on the agent.
11.0	10.x	10.x	Policy and configuration updates cannot be sent to the Endpoint Servers or the agents. Incidents are created based on policy settings before the Enforce Server was upgraded to version 11.0. Incidents are sent to the Enforce Server. If you reboot the Endpoint Server, all policy and configuration information is lost.

About the requirement for language pack upgrades

Symantec Data Loss Prevention requires version-specific language packs. The upgrade process removes all older language packs and rolls the user interface back to the English-language default. After the upgrade, you must download and add new versions of each language pack as needed. See the *Symantec Data Loss Prevention Administration Guide* for information about acquiring and adding updated language packs.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 34.

Upgrade requirements and restrictions

The following are known requirements for performing and upgrade, and known issues that can occur when you upgrade Symantec Data Loss Prevention:

- If your Symantec Data Loss Prevention installation currently uses Symantec DLP 9.x Agents or earlier, you must update those agents to version 10 before you upgrade Endpoint Prevent detection servers to version 11.0. Symantec DLP 9.x and earlier version agents are not compatible with version 11.0 detection servers.
  See "Supported upgrade backward compatibility for agents and servers" on page 37.
- To complete the upgrade, you must have access to the Oracle sys account. Either obtain the sys account password or work with your database administrator to complete the required changes to the Oracle database account before you upgrade.
  See "Preparing the Oracle database for a Symantec Data Loss Prevention upgrade" on page 41.
- You must upgrade all Symantec DLP Agent software to version 10.x before you upgrade Endpoint Prevent detection servers to version 11.0.
  See "Supported upgrade backward compatibility for agents and servers" on page 37.
- You must stop all Network Discover scans before you upgrade the Enforce Server to version 11. You cannot restart Network Discover scans until at least one Network Discover detection server has been upgraded to version 11.
- If a version 10.x detection server stops (shuts down) after you have upgraded the Enforce Server to version 11, you must upgrade that detection server to version 11 before it can restart.
- After you upgrade the Enforce Server to version 11, any configuration changes that you make have no effect on version 10.x detection servers.
- After you complete the upgrade, do not modify the hostname or IP address of a detection server to point to a different detection server. Detection servers use the original configured IP address or hostname to maintain and report server-level statistics.
- The new version numbers for the upgraded detection servers do not show up in the Enforce Server administration console until the Vontu Monitor Controller service has been restarted. The service does not start until the upgrade is complete. Therefore, you cannot check the versions of the upgraded detection

servers in the Enforce Server administration console until the Vontu Monitor Controller service has been restarted.

- When you log on to the Enforce Server after an upgrade, the initial page in the dashboard might appear blank. It also might appear as a cached version 10.x logon page. Either clear your browser cache or press the F5 key on the keyboard to refresh the page.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 34.

About choosing an upgrade method

You can upgrade a system from one version of Symantec Data Loss Prevention to another in two ways:

- Through the Upgrade Wizard, which you access through the Enforce Server. The Upgrade Wizard provides the easiest and most efficient way to upgrade Symantec Data Loss Prevention.
  See "Performing an upgrade with the Upgrade Wizard" on page 49.
- Locally (in other words, manually) on individual detection servers.
  You can upgrade a detection server manually in the following cases:
  - If a detection server was disconnected from the network.
  - If the Vontu services of a detection server were shut down at the time you upgraded the Enforce Server, using the Upgrade Wizard.
  - If the detection server is running on a different operating system from the Enforce Server. The Upgrade Wizard only recognizes detection servers running on the same operating system as the Enforce Server.
    See "About upgrading installations with mixed operating systems" on page 36.
    See "Locally upgrading a detection server" on page 52.

See "About preparing to upgrade Symantec Data Loss Prevention" on page 34.

Preparing your system for the upgrade

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

See "Upgrade requirements and restrictions" on page 39.

See "Preparing the Oracle database for a Symantec Data Loss Prevention upgrade" on page 41.

See "About upgrading the detection servers" on page 42.

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

See "About the minimum system requirements for upgrading to the current release" on page 36.

Preparing the Oracle database for a Symantec Data Loss Prevention upgrade

The following Oracle-related preparations must be made before you use the Upgrade Wizard to upgrade the Symantec Data Loss Prevention database schema for version 11.0:

- Do not upgrade your Oracle 10.2.0.4 database to Oracle 11g before you upgrade to Symantec Data Loss Prevention 11.0. You may choose to upgrade to Oracle 11g after the upgrade to ensure continued security patches. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* for more information.
- You must back up the Oracle database before the upgrade. You cannot recover from an unsuccessful upgrade without a backup of your Oracle database. See the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide* for information on how to back up the database.
- You must add specific permissions to the Symantec Data Loss Prevention database user before you can upgrade to Symantec Data Loss Prevention 11.0. See "Adding permissions to the Enforce Server database account" on page 41.
- Make note of the location of the Oracle home directory on your Enforce Server (this directory is needed later). The home directory is the directory for the installation of the Oracle client tools. This directory functions as the local client installation directory when Enforce uses a remote database. The remote database can be running on Linux, Windows, or any other operating system that the Oracle database can run on. If you installed Oracle 10g using the default options, then the Oracle home is `/opt/oracle/product/10.2.0/db_1` If you installed Oracle 11g, the default Oracle home is `/home/oracle/app/oracle/product/11.2.0/dbhome_1`.

See "Preparing your system for the upgrade" on page 40.

Adding permissions to the Enforce Server database account

Symantec Data Loss Prevention version 11 requires additional database permissions for the Oracle database user that maintains the Enforce Server

database (by default, the “protect” user). You must add these permissions to the database user account before you run the Symantec Data Loss Prevention Upgrade Wizard.

Note: If you create a new database using the Symantec Data Loss Prevention database template, these permissions are granted automatically when you create the protect user. See the *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*.

To add required permissions to an existing protect database account

1 Start SQL*Plus and connect using the sys account:

```
sqlplus /nolog
connect sys/password@protect as sysdba
```

Replace *password* with the password of the sys user.

2 Issue the commands to grant the additional, required permissions:

```
grant execute on dbms_lock to protect;
grant execute on dbms_session to protect;
grant select on v_$sql to protect;
grant select on v_$sql_plan to protect;
grant select on v_$sql_plan_statistics_all to protect;
```

In these commands, replace `protect` with the name of the Oracle user for the Enforce Server database.

About upgrading the detection servers

Prepare for upgrading your detection servers by reviewing the following prerequisites:

- Make sure that the Vontu services on each detection server are running before you start the upgrade.
  See “Verifying that the Enforce Server and the detection servers are running” on page 48.
- Your detection servers must be at Symantec Data Loss Prevention version 10.0 or later. Older versions are not compatible with the version 11.0 Enforce Server.
- Before performing an upgrade using the Upgrade Wizard, verify that all the detection servers to be upgraded are connected.

If a detection server is disconnected when you upgrade the Enforce Server using the Upgrade Wizard, you can upgrade it at a later time by re-running the Upgrade Wizard, or by performing a local (manual) upgrade.

- Before locally upgrading any detection server, you must run the Upgrade Wizard to upgrade the Enforce Server.
- If you have servers running on a different operating system than the Enforce Server, or servers with low-bandwidth connections, upgrade them locally.
- Make sure that all Network Discover scans are halted before starting the upgrade.

See "Preparing your system for the upgrade" on page 40.

About detection server upgrade restrictions

Detection server upgrades have the following restrictions:

- You cannot use the Upgrade Wizard to upgrade a detection server if it is on a different operating system from the Enforce Server. You must instead upgrade the detection server locally.
  The Upgrade Wizard can only automatically upgrade detection servers on the same operating system as the Enforce Server. Linux detection servers that are connected to a Windows Enforce Server must be upgraded locally. Similarly, Windows detection servers that are connected to a Linux Enforce Server must also be upgraded locally.
  See "About upgrading installations with mixed operating systems" on page 36.
- You cannot upgrade a detection server from a version that is older than 10.0 using the Symantec Data Loss Prevention 11.0 Upgrade Wizard. If you have a detection server that is older than 10.0, first perform a local upgrade of that detection server to 10.0. You can then use the Upgrade Wizard to upgrade the detection server to 11.0.

See "Verifying that the Enforce Server and the detection servers are running" on page 48.

See "Preparing your system for the upgrade" on page 40.

Chapter 3

Upgrading Symantec Data Loss Prevention to a new release

This chapter includes the following topics:

Upgrading Symantec Data Loss Prevention

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

Table 3-1 Upgrading Symantec Data Loss Prevention

Step	Action	Description
Step 1	Download and extract the upgrade software.	See "Downloading and extracting the upgrade software" on page 46.
Step 2	(Optional) Specify the Upgrade Wizard port number.	See "Setting the Upgrade Wizard port number" on page 47.
Step 3	Make sure that the Enforce Server and those detection servers on the same operating system are running.	See "Verifying that the Enforce Server and the detection servers are running" on page 48.
Step 4	Launch the Upgrade Wizard on the Enforce Server.	See "Launching the Upgrade Wizard on the Enforce Server" on page 48.
Step 5	Complete the Upgrade Wizard steps.	See "Manually starting the Upgrade Wizard" on page 73.
Step 6	(Optional) Update Endpoint Symantec DLP Agents.	See "About Symantec DLP Agent major version upgrades" on page 55.
Step 7	(Optional) Update any scanners.	See "Upgrading your scanners" on page 54.

Downloading and extracting the upgrade software

Download *Acquiring Symantec Data Loss Prevention Software* from Symantec File Connect after registering your serial number certificates at the Licensing Portal. Follow the directions in that document to acquire the Symantec Data Loss Prevention software.

Download the ZIP file named `Symantec_DLP_11.0_Upgrader_Linux.zip`.

Copy the ZIP file onto the computer from which you intend to perform the upgrade. That computer must have a reliable network connection to the Enforce Server.

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

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

To extract the ZIP file

1. Extract the contents of the ZIP file you downloaded. You may use the `unzip` command to extract the contents of ZIP and JAR files. Among other items, the ZIP file contains an upgrade JAR (Java archive) file, which is required later when you run the Upgrade Wizard. The upgrade JAR file is named `11.0_Upgrader_Linux.jar`.
2. Make note of the directory where the upgrade JAR file is located for later use.

By default the Symantec Data Loss Prevention software is installed in the directory `/opt/Vontu`. Symantec Data Loss Prevention documentation assumes that software is installed in the default directories.

See "Setting the Upgrade Wizard port number" on page 47.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Setting the Upgrade Wizard port number

The Upgrade Wizard has its own default port number, which is 8300. If your organization reserves that port for another purpose, you can reconfigure the Upgrade Wizard to use another port.

To use another port, add one line to the Manager.properties file under `/opt/Vontu/Protect/config`.

In the following line of code, *port* equals the number of the port you want the Upgrade Wizard to use:

```
update.wizard.port=port
```

For example, the following line of code would configure the Upgrade Wizard to use port 5555:

```
update.wizard.port=5555
```

Note: On Linux systems, the port number must always be greater than 1024.

The port number you use must be unique. Another application on the Enforce Server cannot use the same port. Also, if you plan to access the Upgrade Wizard from a different computer from the one where the Enforce Server resides, make sure that firewalls do not block the chosen port.

See "Verifying that the Enforce Server and the detection servers are running" on page 48.

See "Upgrading Symantec Data Loss Prevention" on page 45.

Verifying that the Enforce Server and the detection servers are running

Verify that the Enforce Server is running.

Check that all of the detection servers to be upgraded using the Upgrade Wizard are running the appropriate Vontu services.

See "About Enforce Server services" on page 65.

Although it is easier to upgrade all the servers at the same time using the Upgrade Wizard, you can upgrade individual detection servers later, if needed. If a detection server is disconnected when you first run the Upgrade Wizard, you can re-run the Upgrade Wizard to upgrade the server, or you can perform a local server upgrade. If a detection server is running on a different operating system from Enforce, you must use the local upgrade process to upgrade that server.

To ensure that the detection servers are running

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

See "Launching the Upgrade Wizard on the Enforce Server" on page 48.

See "Upgrading Symantec Data Loss Prevention" on page 45.

Launching the Upgrade Wizard on the Enforce Server

Before launching the Upgrade Wizard, review the following prerequisites and restrictions:

- Make sure that the JAR file you extracted earlier when you performed the upgrade prerequisite steps is available.
  See "Downloading and extracting the upgrade software" on page 46.
- If your installation uses FIPS encryption, your browser will not be able to redirect from the Enforce Server Administration Console to the Upgrade Wizard user interface. In this case, you must manually browse to https://*Enforce_server*:8300.

To launch the Upgrade Wizard

1. Ensure that all detection servers are running and are connected to the Enforce Server.

   See "About Enforce Server services" on page 65.
2. Log on to your Enforce Server.

3 Go to **System > Servers > Overview**.

4 Click **Upgrade**.

The **Upgrade System** pop-up window appears.

5 From the directory in which you extracted the upgrade JAR file, select the file and click **Open**.

6 Click **Launch Upgrade**.

It may take several minutes for the **Symantec Data Loss Prevention Upgrader Login** panel to appear.

If the Enforce Server returns an error, or times out, you must correct the problem before continuing.

See "About troubleshooting Symantec Data Loss Prevention upgrade problems" on page 72.

If no error occurs, the **Symantec Data Loss Prevention Upgrader Login** panel appears and you are ready to continue the upgrade.

See "Performing an upgrade with the Upgrade Wizard" on page 49.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Performing an upgrade with the Upgrade Wizard

Should you encounter an error at any point during the upgrade, examine the log files.

To view the log files

1 On the page where you encountered the error, click the **Log Files** link.

2 Try to resolve the error, and then launch the Upgrade Wizard again.

These procedures assume that you have already launched the Upgrade Wizard.

See "Launching the Upgrade Wizard on the Enforce Server" on page 48.

To upgrade the Enforce Server

1 On the **Symantec Data Loss Prevention Upgrader Login** panel, enter the `Administrator` user name and password, and then click **logon**.

The **License Agreement** panel appears.

2 Click **Accept**.

The **System Check** panel appears. When you click **Next**, the Upgrade Wizard verifies that you have the minimum software version level required to upgrade to the current release version.

3 Click **Next.**

One of the following two outcomes results:

- If the check was successful, the **System Check Succeeded** panel appears.
- If at any point you see a message box stating that the upgrade has failed, click **Cancel**. Fix the reported problem that is shown in the panel. After fixing the problem, log onto Enforce, and launch the upgrade again.

4 From the **System Check Succeeded** panel, click **Next**.

The **Welcome to Symantec Data Loss Prevention Upgrader** panel appears.

5 In the **Oracle home directory** field, enter its path and click **Next**. If you installed Oracle 10g with the default options, then the directory is `/opt/oracle/product/10.2.0/db_1`. If you installed Oracle 11g with the default options, the directory is `/home/oracle/app/oracle/product/11.2.0/dbhome_1`.

6 From the **Upgrade Enforce Server** panel, click **Next**.

The wizard creates a backup ZIP file, called `VontuEnforceBackup.zip`, of all the files in your file system. It puts the ZIP file in a new update directory (`opt/Vontu/Protect/updates`). Then it installs new ones.

This step also upgrades the Symantec Data Loss Prevention schema on the Oracle database.

When the process has finished successfully, the following message appears:

```
Done upgrading Enforce software.
```

If an error occurs, a message to that effect appears. Consult the logs for information, correct the problem, and launch the upgrade again.

Note: If you launch the Upgrade Wizard again to upgrade the remaining detection servers, the utility does not repeat the Enforce Server upgrade.

---

7 Click **Next** after the Enforce upgrade completes.

The **Upgrade Detection Servers** panel appears.

8 Select the detection servers you want to upgrade, or select all servers, then click **Upgrade**.

The wizard creates a backup ZIP file, called `VontuDetectionBackup.zip`. This ZIP file contains all of the files in your file system. It puts the ZIP file in a new update directory (`/opt/Vontu/Protect/updates`). Then it installs new ones.

After the wizard upgrades the detection servers you selected, green checkmarks appear next to those servers listed in the **Upgrade Status** column of the panel. Enforce and the detection servers are operational.

If you experienced network connectivity problems between your Enforce Server and any detection server, you can locally upgrade those servers later. You can also run the Upgrade Wizard again.

See "Locally upgrading a detection server" on page 52.

Note: When you run the Upgrade Wizard again, it does not upgrade the Enforce Server again.

You must upgrade the Enforce Server before trying to upgrade your detection servers. Otherwise, you receive an error message in the system events report and the upgrade does not proceed.

Any detection servers that you do not upgrade to the same version as the newly upgraded Enforce Server will be incompatible with it.

9 Click **Next**.

The **Success** panel appears and prompts you to run the root script.

10 Log on as root to the Enforce Server and to each detection server that you have upgraded. Then go to the `/opt/Vontu/Protect/install/11.0_Upgrade_Resources` directory and run the following script:

```
./11.0_upgrade_root_script.sh
```

This script does the following:

- On the Enforce Server, the script places the new Uninstaller in the correct directory.
- On a detection server, the script sets the correct permissions for packet capture. It also places the new Uninstaller in the correct directory, and it starts the VontuMonitor service.

11 Log on to the Enforce Server.

The Enforce Server administration console appears.

12 To verify that all of your Symantec Data Loss Prevention products are licensed for the current release, navigate to **System > Settings > General**.

If necessary, you can enter additional license files by clicking **Configure** on this page.

For more information, see the *Symantec Data Loss Prevention Administration Guide*.

To verify the upgrade, review that your server version numbers are correct. Go to **System > Servers > Overview** and click Enforce Server or a detection server.

Note: The new version numbers for the upgraded detection servers do not show up in the Enforce Server administration console until the `Vontu Monitor Controller` service has been restarted. The service does not start until the upgrade is complete. Therefore, you cannot check the versions of the upgraded detection servers in the Enforce Server administration console until the `Vontu Monitor Controller` service has been restarted.

Alternatively, on the Enforce Server, go to `/opt/Vontu/Protect/` and check Manager.ver. To check on the detection server, go to the same directory and check Monitor.ver.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Locally upgrading a detection server

You can locally upgrade a detection server if it was disconnected from the network or its Vontu services were shut down at the time you upgraded the Enforce Server.

The Upgrade Wizard can only upgrade detection servers with the same operating system as the Enforce Server. Therefore, any detection servers running on a different operating system from the Enforce Server also need to be upgraded locally.

See "About upgrading the detection servers" on page 42.

Note: Upgrade the Enforce Server before performing local upgrades on detection servers.

To locally upgrade a detection server

1. As the root user, open a command prompt window.
2. Switch to the Symantec Data Loss Prevention system user by entering `su - protect`.
3. Go to the `/opt/Vontu/Protect/updates` directory on the detection server.
4. If it does not already exist, create a directory within `/opt/Vontu/Protect/updates` named `detectionupgrade11.0`. The directory name cannot contain spaces.
5. Copy the 11_0DetectionUpgradePackage.jar file from the `/opt/Vontu/Protect/updates/enforceupgrade11.0` directory on the Enforce Server to the `/opt/Vontu/Protect/updates/detectionupgrade11.0` directory on the detection server. If you manually uploaded the upgrade JAR to the Enforce Server, the upgrade directory is `/opt/Vontu/Protect/updates/enforceupgrade11.0`. If you automatically uploaded the file, the directory is `/opt/Vontu/Protect/updates/update-id-`*x* where *x* is a number based on the time the last upgrade was performed. You should go to the directory with the most recent modification time.
6. Extract the contents of the JAR file into the `/opt/Vontu/Protect/updates/detectionupgrade11.0` directory using the `unzip` command.

   Make sure the files extract to the correct directory. The `start_local_upgrade.sh` file must be in the `/opt/Vontu/Protect/updates/detectionupgrade11.0` directory before you can run it successfully.
7. Change the permissions on the .sh files in the `detectionupgrade11.0` directory by entering `chmod -R a+x *.sh`.
8. Run the file named start_local_upgrade.sh.

   ```
   ./start_local_upgrade.sh
   ```

   To run the utility in command-line text mode, use the -c option:

   ```
   ./start_local_upgrade.sh -c
   ```

9 Follow the options as they appear on the panel. Make sure that the destination directory is set to the `detectionupgrade11.0` directory.

10 Log on as root and, from the `/11.0_Upgrade_Resources` directory, run the 11.0_upgrade_root_script.sh. script on each detection server you have locally upgraded:

```
cd /opt/Vontu/Protect/install/11.0_Upgrade_Resources/
11.0_upgrade_root_script.sh
```

The script corrects permissions that require root privileges to change.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Upgrading your scanners

If you have any version 10.0 scanners, you should upgrade them to Symantec Data Loss Prevention version 11.0 scanners. To upgrade a scanner, remove the older software and then install the Symantec Data Loss Prevention 11.0 scanner.

See the *Symantec Data Loss Prevention Administration Guide* for information on adding and removing scanners.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Upgrading Endpoint Prevent group directory connections

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

See the *Symantec Data Loss Prevention System Administration Guide* for information about creating group directory connections and scheduling directory server indexing.

Chapter 4

Upgrading Symantec DLP Agents

This chapter includes the following topics:

About Symantec DLP Agent major version upgrades

You can upgrade Symantec DLP Agent from one major version to another through the Symantec Management Console, an unattended upgrade process, or you can update the agents manually. Major version upgrades are upgrades from one whole version to another. For example, Upgrading from 10.x to 11.0 is a major upgrade. Manual upgrades are not recommended for large deployments. You can upgrade Symantec DLP Agents as a group if you upgrade using the Symantec Management Console or systems management software. If you upgrade the agents manually, you must upgrade the agents individually.

Endpoint Servers are backward-compatible for one full release with an associated Symantec DLP Agent. For example, you may have a version 11.0 Endpoint Server and a version 10.x Symantec DLP Agent. These versions are compatible.

However, you cannot have an Endpoint Server that runs on version 11.x and a Symantec DLP Agent that runs version 9.x. These two versions are not compatible because they are more than one full release version apart.

See the *Symantec Management Platform User's Guide* for more information on how to download upgrade packages.

After you upgrade the agents to the latest version, the DLP Agent must re-connect to the Endpoint Server before detection resumes. The upgrade process deletes all

stored policy configurations from the Symantec DLP Agent. After the agents re-connect to the Endpoint Server, the agents download the relevant policies.

The following process describes a general overview of the upgrade process:

Table 4-1 Upgrade process for Symantec DLP Agents

Step	Description	Process
Step 1	Download the Symantec DLP Agent upgrade package.	Download the upgrade package from Symantec FileConnect. See the *Symantec DLP Upgrade Guide* for more details.
Step 2	Install the upgrade package on your endpoint computers.	Choose one of the following installation methods: ■ See "Upgrading the Symantec DLP Agent with Symantec Management Console" on page 56. ■ See "Upgrading the Symantec DLP Agent through unattended upgrades" on page 57. ■ See "Upgrading the Symantec DLP Agent manually" on page 58.
Step 3	Restart the Symantec Agents to apply the most current policies.	

Upgrading the Symantec DLP Agent with Symantec Management Console

After you have downloaded the upgrade package into the Symantec Management Console, use the Symantec Management Console to upgrade Symantec DLP Agents on endpoint computers.

Note: If the Symantec DLP Agent fails to upgrade, the agent automatically retries to upgrade the next time it is restarted. The agent only automatically retries to upgrade once. Because of this automatic retry, the agent upgrade may take longer than expected.

To Upgrade Symantec DLP Agents

1. On the DLP Portal page, click the **Upgrade Symantec DLP Agent** link.
2. In the right-hand pane, make sure that the Program name field is set to **Upgrade DLP Agent**.
3. On the top right portion of the page, click the red **Off** icon and select the green **On** icon from the drop-down menu.
4. Under the **Applied to** section, select the **Apply to > Computers** menu option. Add filter rules as necessary to select a subset of endpoint computers.

   The Symantec DLP Agent is upgraded only on the endpoint computers listed.
5. Click **OK**.
6. If you want to schedule the upgrade for a later time, specify those settings in the Schedule section.
7. Click **Save changes**.

If you upgrade between two major releases of the Symantec DLP Agent, you do not need to restart your endpoint computer. However, if you upgrade between a minor release of the Symantec DLP Agent, you must restart your endpoint computer to enable the changes. For example, if you upgrade from version 10.5 to version 11.0, you do not need to restart your endpoint computer. Moving from version 10.5 to version 11.0 is a major version upgrade. If you upgrade from version 10.0 to version 10.5, you must restart your endpoint computer. Moving from version 10.0 to version 10.5 is a minor version upgrade.

Upgrading the Symantec DLP Agent through unattended upgrades

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

To perform an unattended upgrade

1. In your systems management software package, specify the AgentInstall.msi or AgentInstall64.msi package.
2. Specify the AgentInstall.msi installation properties.
3. Specify the `msiexec` properties.
4. Specify any optional properties for the `msiexec` utility.

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

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

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

ENDPOINTSERVER="epserver:8001" SMC="smcserver"

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

In this command:

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

`/i` specifies the name of the package.

`/q` specifies a silent install.

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

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

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

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

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

See "About Symantec DLP Agent major version upgrades" on page 55.

Upgrading the Symantec DLP Agent manually

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

To install Symantec DLP Agent manually

1 Delete the previous version of the Symantec DLP Agent.

You must delete the previous version of the agent before you can upgrade to the newest version.

2 Copy the AgentInstall.msi or AgentInstall64.msi file from the upgrade download site to your endpoint computer and double-click the file.

The Symantec DLP Agent installation wizard starts up, displaying the Symantec DLP Agent setup panel.

3 Click **Next** to accept the copyright agreement.

4 Click **Next** to accept the license agreement.

5 Type the appropriate values in the following fields:

- Endpoint Servers (required)
  Enter the hostname or IP address of at least one Endpoint Server. For example, server.company.com. This value must be consistent with the **Agent Listener > Bind Address (Host/IP)** value you set for the Endpoint Server on the **Symantec Data Loss Prevention Enforce Server > Configure Server page**. If you use a non-default port number, specify it after the server name. For example, server.company.com:8001.
- Encryption Key (optional)
  You may enter a custom authentication key that the Symantec DLP Agents and Endpoint Server use to establish a secure connection. Agents include a default authentication key, but you can also create your own key using the `endpointkeytool` utility. To use your own key, specify it with the `KEY` parameter during deployment and installation. If you decide to use a custom key after installing Symantec DLP Agents, you must reinstall the Symantec DLP Agents to specify the key.
- DLP Agent Service Name (optional)
  You may edit the Symantec DLP Agent service name that appears in the service list of the endpoint computer.
- DLP Watchdog Service Name (optional)
  You may edit the watchdog service name that appears in the service list of the endpoint computer.

6 Click **Next**.

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

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

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

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

9 Click **Finish**.

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

The Symantec DLP Agent now monitors the endpoint.

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

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

About Symantec DLP Agent minor version upgrades

You can upgrade Symantec DLP Agent from one minor version to another through the Symantec Management Console, an unattended upgrade process, or you can update the agents manually. Minor version upgrades are upgrades from one minor version to another. For example, upgrading from 10.0 to 10.5 is a minor upgrade. Manual upgrades are not recommended for large deployments. You can upgrade Symantec DLP Agents as a group if you upgrade using the Symantec Management Console or systems management software. If you upgrade the agents manually, you must upgrade the agents individually.

Endpoint Servers are backward-compatible for one full release with an associated Symantec DLP Agent. For example, you may have an Endpoint Server that is at version 11.0 and a Symantec DLP Agent that is at version 10.x. These versions are compatible.

However, you cannot have an Endpoint Server that is at version 11.x and a Symantec DLP Agent at version 9.x. These two versions are not compatible because they are more than one full release version apart.

See the *Symantec Management Platform User's Guide* for more information on how to download upgrade packages.

After you upgrade the agents to the latest version, the DLP Agent must re-connect to the Endpoint Server before detection resumes. The upgrade process deletes all stored policy configurations from the Symantec DLP Agent. After the agents re-connect to the Endpoint Server, the agents download the relevant policies.

Upgrading the Symantec DLP Agent during a minor version release involves different steps than the process for upgrading the agents during a major version

release. Unlike upgrading during a major release, agent upgrades for minor releases use the `Agent_Install.bat` script to upgrade the agents.

By default, the agent upgrade script is stored in the following directory:

```
c://Program Files/Manufacturer/Agent Install/Scripts
```

You will need to access the script to upgrade your agents.

See "Upgrading minor version agents with Symantec Management Console" on page 61.

See "Upgrading minor version agents through unattended upgrades" on page 61.

See "Upgrading minor version agents manually" on page 62.

Upgrading minor version agents with Symantec Management Console

To upgrade minor version Symantec DLP Agents with Symantec Management Console

1. From the SMC left-hand navigation window, go to: **Data Loss Prevention Portal > Configuration > V11.0 Agent Deployment > DLP Agent Package**.
2. Click the **Programs** tab.
3. In the Command line filed, replace the command with the following script:

   ```
   msiexec /i AgentInstall.msi \q REOMSTA::=ALL REINSTALLMODE=vomus
   ```
4. Click **Save Changes**.
5. On the left-hand navigation, click the **Upgrade Agent** link.
6. Run the task.

See "About Symantec DLP Agent minor version upgrades" on page 60.

Upgrading minor version agents through unattended upgrades

To upgrade minor version Symantec DLP Agents with unattended upgrades

1. Open the Agent_Upgrade script.
2. Modify the script to your specifications.
3. Run the script through your systems management software.

See "About Symantec DLP Agent minor version upgrades" on page 60.

Upgrading minor version agents manually

To upgrade minor version Symantec DLP Agents manually

1. Open a command window on the endpoint computer you want to upgrade.
2. Navigate to the Scripts folder. Usually `<dir> Program Files/Manufacturer/Endpoint Agent/Scripts.`
3. Enter the name of the upgrade script: Agent_upgrade.bat.
4. Press Enter.

See "About Symantec DLP Agent minor version upgrades" on page 60.

Chapter 5

Post-upgrade tasks

This chapter includes the following topics:

Performing post-upgrade tasks

You must perform certain tasks after you finish upgrading.

See "Verifying Symantec Data Loss Prevention operations" on page 63.

See "Turning on VEP file optimization" on page 64.

See "Symantec Data Loss Prevention upgrade phases" on page 34.

Verifying Symantec Data Loss Prevention operations

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

To verify Symantec Data Loss Prevention operations

1. Log on to the Enforce Server administration console as Administrator.
2. Log out of the Enforce Server administration console and then log on as a user other than Administrator.
3. Go to the **System Overview** screen and recycle the detection servers to verify that they are connected.
4. Click on each heading in the Enforce Server navigation pane to view the data that was carried over from the previous version.

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

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

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

8 If you use Lookup plug-ins, confirm that the Plugins.properties file in the `/opt/Vontu/Protect/config` directory has its lookup configuration information.

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

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

See "Performing post-upgrade tasks" on page 63.

Turning on VEP file optimization

VEP file optimization lets you increase USB file transfer performance. The VEP setting optimizes the way that files are transferred to or from a USB-connected device. Turn on VEP file optimization if the following conditions are all true:

- Your Symantec Data Loss Prevention installation does not use data retention policies.
- Your Symantec Data Loss Prevention installation does not use two-tier detection policies.
- You have not installed Symantec Endpoint Encryption software.

VEP file optimization can be turned back on with an advanced Enforce Server setting.

See the Symantec Data Loss Prevention online Help for more information regarding Endpoint advanced settings.

Chapter 6

Starting and stopping Symantec Data Loss Prevention services

This chapter includes the following topics:

About Enforce Server services

The Symantec Data Loss Prevention services may need to be stopped and started periodically. This section provides a brief description of each service and how to start and stop the services on supported platforms.

The Symantec Data Loss Prevention services for the Enforce Server are described in the following table:

Table 6-1 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.
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 66.
- See "Stopping an Enforce Server on Linux" on page 66.
- See "Starting a detection server on Linux" on page 67.
- See "Stopping a detection server on Linux" on page 67.
- See "Starting services on single-tier Linux installations" on page 68.
- See "Stopping services on single-tier Linux installations" on page 68.

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 66.

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 66.

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 67.

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 67.

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 68.

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 68.

Chapter 7

Symantec Data Loss Prevention upgrade troubleshooting and recovery

This chapter includes the following topics:

About troubleshooting Symantec Data Loss Prevention upgrade problems

If you experience problems either with launching the Upgrade Wizard or with completing a successful product upgrade, see these topics:

- See "Troubleshooting Upgrade Wizard launch problems" on page 72.
- See "Reverting to the previous Symantec Data Loss Prevention release" on page 74.

Troubleshooting Upgrade Wizard launch problems

Occasionally, after trying to launch the Upgrade Wizard on the Enforce Server, you may observe a timeout or other error. This error can occur for several reasons:

- The upgrade JAR file failed to upload properly.
  See "Correcting JAR file upload problems" on page 72.
- If you receive the following error message, FIPS encryption is most likely enabled for your installation:

  `"Unable to send redirect. System update did not succeed"`

  This means that your browser cannot redirect from the Enforce Server Administration Console to the Upgrade Wizard user interface. In this case, you must manually browse to https://*Enforce_server*:8300.

Correcting JAR file upload problems

Occasionally, the upgrade JAR file fails to load correctly. This failure may result in a timeout of the Upgrade Wizard launch or another error.

Use one of the following methods to address JAR file upload errors:

- Browse to the Upgrade Wizard URL:

  `https://Enforce_server:8300`

  where *Enforce_server* is the name of your Enforce Server. If you have changed the default port from 8300, use your new port instead.
- Click **Upgrade** again and repeat the upload of the upgrade JAR file.

If neither method works, then you must manually upload the JAR file to the Enforce Server.

See "Manually uploading the JAR file to the Enforce Server" on page 73.

Manually uploading the JAR file to the Enforce Server

If you encounter an error, such as a timeout, when uploading the upgrade JAR file to your Enforce Server, then upload the JAR file manually.

To manually upload the JAR file to the Enforce Server

1. As the root user, copy the upgrade JAR file `11.0_Upgrader_Linux.jar` to the `/opt/Vontu/Protect/updates` directory. Change the owner of the file to the Symantec Data Loss Prevention system user (by default, the user is named protect) using the following command:

   ```
   chown protect:protect 11.0_Upgrader_Linux.jar
   ```

2. Switch to the Symantec Data Loss Prevention system ("protect") user by entering `su - protect`.
3. Change to the `/opt/Vontu/Protect/updates` directory.
4. Create a new directory that is named `enforceupgrade11.0` inside the `/opt/Vontu/Protect/updates` directory by entering: `mkdir enforceupgrade11.0`.
5. Extract the contents of the Upgrade JAR file 11.0_Upgrader_Linux.jar into the `enforceupgrade11.0` directory.

   Go to the `enforceupgrade11.0` directory (`cd enforceupgrade11.0`). Run the command `unzip ../11.0_Upgrader_Linux.jar`.
6. Change the permissions on the sh files in the `enforceupgrade11.0` directory by entering `chmod a+x *.sh`.

You may now manually start the Upgrade Wizard.

See "Manually starting the Upgrade Wizard" on page 73.

Manually starting the Upgrade Wizard

Follow this procedure if you must manually start the Upgrade Wizard.

To manually start the Upgrade Wizard

1. As the Symantec Data Loss Prevention system user (the protect user), run the file named start_upgrade_wizard.sh located in the `/opt/Vontu/Protect/updates/enforceupgrade11.0` directory. You should already be logged on as the protect user and be in the correct directory, so you need to enter `./start_upgrade_wizard.sh`.
2. Wait a few minutes for the Upgrade Wizard server to start.

3 Open a Web browser and go to: `https://Enforce_server:8300`

where *Enforce_server* is the name or IP address of your Enforce Server. If you have changed the default port from 8300, then you use your new port instead. The Web browser displays the Upgrade Wizard logon page.

4 Continue using the standard upgrade procedures.

See "Performing an upgrade with the Upgrade Wizard" on page 49.

Reverting to the previous Symantec Data Loss Prevention release

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

Different procedures are used to roll back single-tier versus two-tier and three-tier installations:

When Symantec Data Loss Prevention is upgraded to a newer release, the upgrade first saves the existing installation in a backup file. The backup file is created as a tar.gz file that resides under `/Vontu/Protect/updates/update-id-X`, where *X* is a number. If a system has been upgraded multiple times, you see multiple `/update-id-X` directories.

- Two- and three-tier systems. When rolling back upgrades on installations with multiple `update-id-X` directories, always use the backup file from the directory with the most recent timestamp.
- Single-tier systems. Single-tier systems always have at least two `update-id-X` directories. One `update-id-X` directory is created during the Enforce Server upgrade. The other `update-id-X` is created during the detection server upgrade. The detection server `update-id-X` directory normally has a later timestamp than the Enforce Server directory.
  Never use any file for this purpose except the backup file that was created during the Enforce Server upgrade to roll back a single-tier installation.

See "Reverting to the previous release in a single-tier installation" on page 75.

See "Reverting to the previous release in a two- or three-tier installation" on page 76.

See "Reverting to the previous release on a detection server" on page 77.

See "Reverting to the previous release on a Linux Enforce Server" on page 78.

Reverting to the previous release in a single-tier installation

In a single-tier installation, the Enforce Server, detection servers, and Oracle database all reside on the same machine. Use the following procedure to roll back a single-tier Symantec Data Loss Prevention installation to the previous release.

To revert to the previous release on a single-tier server

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

   See "About Enforce Server services" on page 65.

2. Stop all the Oracle services.
3. Restore the Symantec Data Loss Prevention database from the latest backup.
4. Restart all the Oracle services.
5. Go to the Enforce-related `Protect/update-id-X` directory with the most recent timestamp.

   To be sure that you are in the correct directory, look for a file named `start_upgrade_wizard.*`, which is only present in the Enforce-related `update-id-X` directory.

   Warning: If you use the detection server backup file, only that upgrade is rolled back, and the Enforce Server remains upgraded.

   See "Reverting to the previous Symantec Data Loss Prevention release" on page 74.

   If you performed the upgrade locally, go to the upgrade subdirectory you created.

   See "Locally upgrading a detection server" on page 52.

6. In the update directory, locate the backup file.

   Backup files use the naming convention `VontuNBackup.tar.gz`, where `N` is a number that signifies the Symantec Data Loss Prevention version that is backed up.

7. Move the backup file to a temporary directory outside of the `Vontu` directory structure, (for example, `/tmp`).

8. Delete the entire contents of the `Vontu` directory and all of its subdirectories. Or, create a compressed archive of the directory and move the contents elsewhere if you want to keep a record of the failed upgrade.
9. Allow the `Vontu` directory to be written to by anyone by entering:

   ```
   chmod a+w /opt/Vontu
   ```

10. Switch to the Symantec Data Loss Prevention system user by entering:

    ```
    su - protect
    ```

11. Extract the contents of the Vontu backup file into the `Vontu` directory.

    Go to the directory where you stored the Vontu backup file and extract its contents into the `Vontu` directory, using the extract permission option (p).

12. Exit back to the root user by entering:

    ```
    exit
    ```

13. Remove the ability for anyone to write to the `Vontu` directory by entering:

    ```
    chmod a-w /opt/Vontu
    ```

14. Set the owner and permissions of the PacketCapture executable by entering:

    ```
    chown root:protect /opt/Vontu/Protect/bin/PacketCapture
    chmod 6750 /opt/Vontu/Protect/bin/PacketCapture
    ```

15. Restart the Vontu services.

See "About Enforce Server services" on page 65.

For more information on single-tier installations, see the *Symantec Data Loss Prevention Installation Guide* for your platform.

See "Reverting to the previous Symantec Data Loss Prevention release" on page 74.

Reverting to the previous release in a two- or three-tier installation

If the Enforce Server and detection servers are on separate computers, roll them back in the following order:

- Detection servers
  See "Reverting to the previous release on a detection server" on page 77.

- Enforce Server
  See "Reverting to the previous release on a Linux Enforce Server" on page 78.

See the appropriate *Symantec Data Loss Prevention Installation Guide* for more information on two-tier installations.

Reverting to the previous release on a detection server

This procedure is only used for two- and three-tier installations.

To roll back an individual detection server to the previous release, perform the following steps:

To roll back a detection server

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

   See "About Enforce Server services" on page 65.

2. Go to the `/opt/Vontu/Protect/updates/update-id-X` directory with the most recent timestamp.

3. In the update directory, locate the backup file.

   Backup files use the naming convention `VontuNBackup.tar.gz`, where `N` is a number that signifies the Symantec Data Loss Prevention version that is backed up.

4. Allow the `Vontu` directory to be written to by anyone by entering:

   ```
   chmod a+w /opt/Vontu
   ```

5. Switch to the Symantec Data Loss Prevention system user by entering:

   ```
   su - protect
   ```

6. Go to the directory where you put the backup file (`/tmp` for example).

7. Extract the contents of the backup file into the `Vontu` directory using the extract permission option (-p). For example, enter:

   ```
   tar xvfPpz backup_filename.tar.gz
   ```

8. Exit back to the root user by entering:

   ```
   exit
   ```

9 Remove the ability for anyone to write to the `Vontu` directory by entering:

```
chmod a-w /opt/Vontu
```

10 Set the owner and permissions of the PacketCapture executable by entering:

```
chown root:protect /opt/Vontu/Protect/bin/PacketCapture
chmod 6750 /opt/Vontu/Protect/bin/PacketCapture
```

11 Restart the Vontu services.

See "About Enforce Server services" on page 65.

See "Reverting to the previous Symantec Data Loss Prevention release" on page 74.

Reverting to the previous release on a Linux Enforce Server

This procedure is only used for two- and three-tier installations.

To roll back an Enforce Server to the previous release, perform the following steps:

To roll back a Linux Enforce Server

1 Log on to the Enforce Server as root and stop all Symantec Data Loss Prevention services.

See "About Enforce Server services" on page 65.

2 Stop all the Oracle services.

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

4 Restart all the Oracle services.

5 Remove, or make a backup of the Protect and /jre directories in the `/Vontu` tree.

6 Create a backup of the `/.install4j` directory inside the `/Vontu` tree.

7 Allow write access to the `Vontu` directory by anyone by entering:

```
chmod a+w /opt/Vontu
```

8 Switch to the Symantec Data Loss Prevention system user by entering:

```
su - protect
```

9 Go to the `/Vontu/Protect/updates/update-id-N` directory with the latest timestamp.

See "Reverting to the previous Symantec Data Loss Prevention release" on page 74.

If you performed the upgrade locally, then go to the upgrade subdirectory you created.

See "Locally upgrading a detection server" on page 52.

10 In the `update-id-N` directory, locate the backup file. This file is named `VontuNBackup.tar.gz` where `N` is a number that signifies the Symantec Data Loss Prevention version that is backed up.

11 Move the backup file to a temporary directory outside of the `Vontu` directory structure; for example, `/tmp`.

12 Delete the `/Vontu/Protect` directory and all of its subdirectories. Alternatively, if you want to keep a record of the failed upgrade, you can create a compressed archive of this directory and move it elsewhere.

13 Go to the directory where you put the backup file (for example, `/tmp`). Extract the backup file content into the `Vontu` directory, using the extract permission flag (p). For example, enter:

```
tar xvfPpz Vontu10.xBackup.tar.gz
```

14 Exit back to the root user.

15 Restore the `/.install4j` directory in the `/Vontu` tree from the backup location.

16 Make sure that this directory is owned by the protect user.

```
chown protect:protect .install4j
```

17 Remove the ability for anyone to write to the `Vontu` directory by entering:

```
chmod a-w /opt/Vontu
```

18 Restart all Vontu services.

See "About Enforce Server services" on page 65.

Index

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X