Symantec™ Data Loss Prevention Release Notes

Version 11.6

Symantec Data Loss Prevention Release Notes

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

Documentation version: 11.6b. Last updated: 13 July, 2012.

Legal Notice

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

Managed Services — These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services — Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

Education Services — Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

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

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Introduction

This chapter includes the following topics:

- About these release notes
- About accessing the Symantec Data Loss Prevention Knowledgebase

About these release notes

This document contains important and late-breaking information about Symantec Data Loss Prevention version 11.6.

Before installing Symantec Data Loss Prevention, refer to the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about system requirements. This guide is available online at the following URL:

https://kb-vontu.altiris.com/article.asp?article=55645

When you are ready to install Symantec Data Loss Prevention, refer to the *Symantec Data Loss Prevention Installation Guide*. Or, if you are upgrading, see the *Symantec Data Loss Prevention Upgrade Guide*.

These release notes are updated periodically. You can view the most current version of these Release Notes at the following URL:

https://kb-vontu.altiris.com/article.asp?article=55642

About accessing the Symantec Data Loss Prevention Knowledgebase

In addition to your product documentation, the Symantec Data Loss Prevention Knowledgebase is a valuable resource for information. The Knowledgebase provides solutions to common problems, troubleshooting tips, and other useful information.

In addition, important product announcements, updated release notes and product guides, and product bulletins are published at the Knowledgebase.

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

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

To create an account

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

It may take several days to process your request.

Chapter 2

What's new

This chapter includes the following topics:

What's new and what's changed for Symantec Data Loss Prevention version 11.6

This topic describes new features and other product changes for Symantec Data Loss Prevention version 11.6. Subsequent topics describe the new features for previous versions of Symantec Data Loss Prevention version 11.x., and are included for users who may be upgrading from earlier versions of Symantec Data Loss Prevention.

This topic includes new features for the following product areas:

- See "New Advanced Reporting Module – Data Loss Prevention IT Analytics" on page 14.

- See "New Oracle database features in version 11.6" on page 14.

- See " New Symantec Data Loss Prevention for Mobile features in version 11.6" on page 14.

- See "New Incident reporting and remediation features in version 11.6" on page 15.

- See "New Network Monitor and Network Prevent features in version 11.6" on page 16.

- See "New Network Discover features in version 11.6" on page 16.

- See "New Endpoint Discover and Endpoint Prevent features in version 11.6" on page 17.
- See "New detection feature in version 11.6" on page 18.

New Advanced Reporting Module – Data Loss Prevention IT Analytics

Data Loss Prevention IT Analytics is a new, free of charge, advanced reporting module that complements and expands upon the reporting capabilities offered by the Enforce Server administration console. It processes and summarizes data from the Data Loss Prevention Oracle database to create extremely fast, multi-dimensional reports across a broad set of Data Loss Prevention data including incidents, repository scans, agents, policy changes, and auditable actions. It provides multi-dimensional analysis and robust graphical reporting features and enables you to summarize data across Data Loss Prevention products and even across multiple Enforce Server platforms. Data Loss Prevention IT Analytics is supported for Symantec Data Loss Prevention version 10.5 and later.

For more information, see the *Data Loss Prevention Pack for Altiris IT Analytics Solution 7.1 SP2 from Symantec User Guide*, available at the following URL:

http://www.symantec.com/business/support/index?page=content&id=DOC5526&key=56005

New Oracle database features in version 11.6

The supported version of Oracle database software for Symantec Data Loss Prevention version 11.6 is Oracle 11g, version 11.2.0.3.

For more information, see the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide*.

New Symantec Data Loss Prevention for Mobile features in version 11.6

Symantec Data Loss Prevention for Mobile replaces Symantec Data Loss Prevention for Tablets and introduces support for Apple iPhones. The Mobile Prevent for Web Server prevents Apple iPads and iPhones with iOS versions 4 and 5 operating systems from transmitting sensitive information. The Mobile Prevent for Web Server scans HTTP, HTTPS, and FTP transmissions from mobile devices. Mobile Prevent secures corporate email when used with Microsoft Exchange ActiveSync. Mobile Prevent enables you to monitor and block mobile-specific incidents, which you can remediate in the Enforce Server administration console.

The Mobile Prevent solution works by routing iPad and iPhone communication through a secure corporate VPN connection. The network connection is maintained through either Wi-Fi or 3G connectivity. After the VPN connection is established, the Mobile Prevent for Web Server applies your security policies to the data that transfers from your mobile devices. You can use a Mobile Device Management (MDM) solution to configure and enforce the VPN configuration.

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

In addition to iPhone support, Symantec Data Loss Prevention for Mobile also supports Gmail ActiveSync in addition to the existing support for Microsoft ActiveSync. The Gmail email account must be added using the Microsoft Exchange account through the native iOS Mail application. Symantec Data Loss Prevention for Mobile can monitor the new email account and block any sensitive emails that are sent using the iOS Mail application.

For more information, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.

New Incident reporting and remediation features in version 11.6

- Email Quarantine Connect
  Email Quarantine Connect is an integration of Symantec Messaging Gateway and Symantec Data Loss Prevention. The integration uses both Symantec Data Loss Prevention and Symantec Messaging Gateway for detection of sensitive messages and enables users to remediate the resulting incidents on either platform. Typically, the integration is intended for a workflow where Symantec Data Loss Prevention applies detection policies to email messages and sends suspect messages to Symantec Messaging Gateway where they are quarantined pending further remediation. Email Quarantine Connect is implemented in Symantec Data Loss Prevention as a Server FlexResponse plug-in.
  For more information, see the *Symantec Data Loss Prevention Email Quarantine Connect FlexResponse Implementation Guide*.

- Incident archiving
  Incident archiving lets you flag specified incidents as "archived." These archived incidents are excluded from normal incident reporting, so you can improve the reporting performance of your Symantec Data Loss Prevention deployment by archiving any incidents that are no longer relevant. The archived incidents remain in the database; they are not moved to another table, database, or other type of offline storage.
  For more information, see the *Symantec Data Loss Prevention System Maintenance Guide*.

- Incident counter
  To improve database performance, you can configure a process on the Enforce Server that runs daily to count the number of incidents in the Enforce Server database. If the count exceeds a configurable threshold, the Enforce Server generates a system event.

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

- Incident Reporting and Update API

  The Symantec Data Loss Prevention Incident Reporting and Update API lets developers create applications that retrieve and update incident data that is stored in a Symantec Data Loss Prevention deployment. You can use this API to integrate incident data with other applications or systems to provide dynamic reporting, create a custom incident remediation process, or to support business processes that rely on Symantec Data Loss Prevention incidents.

  The Incident Reporting and Update API extends the functionality currently available with the deprecated Reporting API to include the ability to update incident data. For backward compatibility, the deprecated Reporting API WSDL is still available for use by Reporting API clients.

  For more information, see the *Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide*.

- Lookup plug-ins

  Incident attribute lookup plug-ins are now configured through the Enforce Server administration console. Authorized users can create, modify, enable, and chain lookup plug-ins from the centralized user interface. In addition, the CSV Lookup Plug-In is upgraded to support the lookup of incident attribute values from large-sized CSV files. Other supported lookup plug-ins include LDAP, Script, and Data Insight. The Custom (Legacy) Lookup Plug-In is preserved for migrating legacy custom Java lookup plug-ins to the new framework.

  For more information, see the *Symantec Data Loss Prevention Administration Guide* and the online Help documentation.

New Network Monitor and Network Prevent features in version 11.6

Network Monitor now supports the Napatech high-speed packet capture adapter for Windows and Linux, 64-bit systems.

For more information, see the *Symantec Data Loss Prevention Administration Guide* and the *Symantec Data Loss System Requirements and Compatibility Guide*.

New Network Discover features in version 11.6

- Updates to the Discover Target List and Scan History pages

  The updated **Discover Target List** page makes it easier to view and manage your Discover scan targets. The new **Scan History** page lets you view and manage information about scans from all your Network Discover scan targets.

- Exchange Web Services crawler

Network Discover can now scan Microsoft Exchange Servers, versions 2007 SP2 and later, using Exchange Web Services. The Exchange Web Services crawler scans Exchange servers directly from the Network Discover sever; you do not need to install a scanner on your Exchange servers.Using the Exchange Autodiscover feature, the crawler fetches Exchange server and mailbox information from Active Directory, and pulls data directly from the appropriate Exchange servers using a Simple Object Access Protocol (SOAP) interface.

- Autodiscovery of file shares
  Network Discover can now automatically discover and crawl open file shares on a specified CIFS server. You specify the UNC path or SMB URL and Symantec Data Loss Prevention automatically finds and scans open file shares on that server.
- Incremental scanning for SharePoint targets
  Network Discover now supports incremental scanning for SharePoint targets.
- New SharePoint solution
  Symantec Data Loss Prevention includes a new SharePoint solution that you must install on your SharePoint Web Front Ends. This version of the SharePoint solution is not backward-compatible.

For more information about all these features, see the *Symantec Data Loss Prevention Administration Guide.*

- SharePoint Quarantine FlexResponse Plug-ins
  The SharePoint Quarantine FlexResponse Plug-in lets you remediate a Network Discover incident by placing a SharePoint 2007 or 2010 document into quarantine in a specified location within your SharePoint site collection. Using the SharePoint Release from Quarantine FlexResponse plug-in, you can release quarantined SharePoint documents from quarantine and return them to their original location. You can use either manual (Smart) or automatic remediation. The SharePoint Quarantine FlexResponse plug-in only works for SharePoint documents, not for content in list items such as Wikis or blogs.

For information about the SharePoint Quarantine FlexResponse Plug-ins, see the *Symantec Data Loss Prevention SharePoint Quarantine FlexResponse Plug-in Implementation Guide.*

New Endpoint Discover and Endpoint Prevent features in version 11.6

- Symantec Data Loss Prevention Endpoint Discover can now be configured to timeout after a specified time period. An Endpoint Discover scan might not complete due to one or more Endpoint computers remaining disconnected from the Endpoint Server. An Endpoint Discover scan can be configured to stop scanning if an Endpoint computer remains offline for a specified amount of time.

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

- Symantec Data Loss Prevention Endpoint Prevent can now detect when sensitive data is transferred to an eSATA removable drive. This ability prevents a user from copying sensitive data to a removable drive that is connected to the eSATA connector on their computer.

  For more information, see the *Symantec Data Loss Prevention Administration Guide*.
- Symantec Data Loss Prevention introduces improved tamper-proofing capabilities for Endpoint computers. A user cannot stop the Symantec DLP Agent which allows Endpoint Prevent to continuously monitor the endpoint computer to prevent the loss of sensitive data.

  For more information, see the *Symantec Data Loss Prevention Administration Guide*.
- Symantec Data Loss Prevention administrators can now configure log level settings for DLP Agents through the Enforce Server administration console. Symantec Technical Support uses the DLP Agent logs to help troubleshoot a problem or to improve system performance.

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

New detection feature in version 11.6

- Unique Match Counting for Data Identifiers

  When implementing a Data Identifier, you can now choose to count only those matches that are unique. For example, with unique match counting enabled, you can create a Data Identifier policy that would block the transmission of a document containing 25 or more unique social security numbers. In this case, the policy would not trigger an incident if the data contained 25 instances of the same social security number. Unique match counting does not replace the default method of counting all matches, thereby providing policy authors greater flexibility.

  For more information, see the *Symantec Data Loss Prevention Administration Guide* and the online Help documentation.

Symantec Data Loss Prevention features and changes for versions 11.0 – 11.5

This topic includes new features and enhancements for Symantec Data Loss Prevention versions 11.0, and 11.1.x for the following product areas:

- See “New installation and upgrade features in versions 11.0 – 11.5” on page 19.
- See “New Enforce Server features in versions 11.0 – 11.5” on page 21.
- See “Symantec Data Loss Prevention for Tablets” on page 22.
- See “New Endpoint features in versions 11.0 – 11.5” on page 22.
- See “New Network Discover and Network Protect features in versions 11.0 – 11.5” on page 24.
- See “New Network Monitor and Network Prevent features in versions 11.0 – 11.5” on page 27.
- See “New detection features in versions 11.0 – 11.5” on page 27.
- See “New report features in versions 11.0 – 11.5” on page 29.
- See “New language support in versions 11.0 – 11.5” on page 29.
- See “New product documentation features in versions 11.0 – 11.5” on page 29.

New features that are specific to Symantec Data Loss Prevention version 11.1 are labeled “(New in v11.1).”

New installation and upgrade features in versions 11.0 – 11.5

Symantec Data Loss Prevention version 11.x offers several new options when you install a new version of the software or upgrade from a previous version:

- Single sign-on configuration (New in 11.1)
  The Symantec Data Loss Prevention installer enables you to configure new single sign-on options when you install an Enforce Server. As an alternative, you can configure these sign-on options after the installation process completes. See the *Symantec Data Loss Prevention Installation Guide* for your platform.
- Automated Server FlexResponse actions (New in 11.1)
  When you upgrade Symantec Data Loss Prevention to version 11.1, any server FlexResponse plug-ins that you have deployed can be used for creating Automated Response Rules as well as Smart Response Rules. This means that you can create policies that automatically apply server FlexResponse plug-in

actions after an incident is created. See the *Symantec Data Loss Prevention Upgrade Guide* for your platform.

- Citrix XenApp 6 and XenDesktop 4 support (New in 11.1)

  Symantec Data Loss Prevention supports deploying the Symantec DLP Agent software directly on Citrix XenApp/Application servers or Citrix XenDesktop virtual machines running on Windows 2008 R2 (64-bit) host computers. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.

- VM support for Endpoint Prevent servers (New in 11.1)

  Symantec Data Loss Prevention supports running Endpoint Prevent detection servers on compatible virtualization products. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for a list of compatible products.

- 64-bit agent support

  Symantec DLP Agent can now operate on compatible 64-bit operating systems. Symantec DLP Agents are supported on the 64-bit versions of Windows Server 2008 R2 or later

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

- 64-bit system support

  Symantec Data Loss Prevention servers can now run in 64-bit mode on Red Hat Enterprise Linux 5 Update 2 or later.

- 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*.

  Note: As of Symantec Data Loss Prevention version 11.5, the supported version of Oracle was 11.2.0.2.

- 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 for Email and Network Prevent for 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 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.x.

New Enforce Server features in versions 11.0 – 11.5

Symantec Data Loss Prevention introduces two new ways for users to authenticate themselves and log onto the Enforce Server administration console:

- Certificate authentication with single sign-on

  Certificate authentication enables a user to automatically log on to the Enforce Server administration console using an X.509 client certificate that is generated by your public key infrastructure (PKI).

- SPC-based authentication with single sign-on

  With SPC integration, a user first logs into the SPC console, and may then access the Enforce Server administration console from within the SPC interface.

You can use these authentication mechanisms in addition to the other authentication mechanisms that Symantec Data Loss Prevention supports, such as password authentication.

The Symantec Data Loss Prevention version 11.1 installation program provides the option to enable either of these authentication mechanisms when you install a new Enforce Server. If you are upgrading an existing Enforce Server to version 11.1, follow the instructions in the *Symantec Data Loss Prevention Administration Guide* to enable certificate authentication or SPC-based authentication.

Symantec Data Loss Prevention for Tablets

Note: In Symantec Data Loss Prevention version 11.6, Symantec Data Loss Prevention for Tablets has been renamed Symantec Data Loss Prevention for Mobile and includes support for iPhones.

See “ New Symantec Data Loss Prevention for Mobile features in version 11.6” on page 14.

The Tablet Prevent detection server prevents Apple iPads with iOS 4 or iOS 5 operating systems from transmitting sensitive information through HTTP, HTTPS, and FTP. Tablet Prevent also secures corporate email when used with Microsoft Exchange ActiveSync. Tablet Prevent enables you to monitor and block Tablet-specific incidents, which you can view in the Enforce Server administration console.

The Tablet Prevent solution works by routing iPad communications through a secure corporate VPN connection. The network connection is maintained through either Wi-Fi or 3G connectivity. After the VPN connection is established, the Tablet Prevent for Web server applies your security policies to the data that is transferring from your iPad devices. You can use a Mobile Device Management (MDM) solution to configure and enforce the iPad VPN configuration.

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

New Endpoint features in versions 11.0 – 11.5

For Endpoint, the following new features are available in version 11.x:

- 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.

- 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 connected v11.x agent that is registered with the Enforce Server administration console.

- Symantec Management Platform version 7.1 support

  The DLP Integration Component is now supported by 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.
- 64-bit Microsoft Outlook 2010 support
  Microsoft Outlook 2010 64-bit is now supported.
- Uninstallation passwords (New in v11.1)
  You can specify that a password be entered before the Symantec DLP Agent can be uninstalled. The password is specified during agent installation or upgrade.
- Microsoft Windows 2008 32-bit and 64-bit support. (New in v11.1)
  32-bit and 64-bit Microsoft Windows 2008 operating system is now supported.
- Citrix XenApp 6 and XenDesktop 4 support (New in 11.1)
  Symantec Data Loss Prevention supports deploying the Symantec DLP Agent software directly on Citrix XenApp/Application servers or Citrix XenDesktop virtual machines running on Windows 2008 R2 (64-bit) host computers. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.
- Virtualized environment support for Endpoint servers (New in v11.1)
  Endpoint Servers are now supported in VMware virtualized environments. See the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*.
- Metadata detection (new in v11.5)
  Symantec Data Loss Prevention Endpoint Agents can now detect policy violations based on metadata. When this feature is enabled, you can detect metadata for Microsoft Office and PDF documents. For Microsoft Office files, Object Linking and Embedding (OLE) metadata is supported, which includes the fields Title, Subject, Author, and Keywords. For PDF files, Document Information Dictionary metadata is supported, which includes fields such as Author, Title, Subject, Creation, and Update dates.
  See the *Symantec Data Loss Prevention Administration Guide* for more information.

New Network Discover and Network Protect features in versions 11.0 – 11.5

For Network Discover and Network Protect, the following new features are available in version 11.x:

- 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.

- SharePoint solution to restrict scans to site collections (new in v11.5.1)

  Symantec Data Loss Prevention includes a new SharePoint solution that allows you to restrict a scan to only the site collections under a specified SharePoint web application URL.

  See "SharePoint solution on the Web Front Ends in a farm" in the *Symantec Data Loss Prevention Administration Guide.*

New Network Monitor and Network Prevent features in versions 11.0 – 11.5

For Network Prevent and Network Monitor, the following new features are available in version 11.x:

- 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 platform support (New as of v 11.5)

  The following platforms are now supported:

  - Websense V-Series Appliance version V10000 proxy server
  - Microsoft Threat Management Gateway (TMG) Server 2010 Standard or Enterprise Edition

  For detailed platform support, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for more information.

New detection features in versions 11.0 – 11.5

Symantec Data Loss Prevention version 11.x offers several new policy detection features.

These new features include:

- Vector Machine Learning (New in 11.1)

  Vector Machine Learning (VML) protects unstructured data by performing statistical analysis to determine if content is similar to an example set of documents you train against. With VML you do not have to locate and fingerprint all of the data you want to protect, nor do you have to describe it and risk inaccuracies. VML simplifies the detection of text-based, sensitive content while offering the potential for high accuracy.

- Automated Server FlexResponse actions (New in 11.1)

  When you upgrade Symantec Data Loss Prevention to version 11.1, any server FlexResponse plug-ins that you have deployed can be used for creating Automated Response Rules as well as Smart Response Rules. This means that you can create policies that automatically apply server FlexResponse plug-in actions after an incident is created. See the *Symantec Data Loss Prevention Administration Guide*.

- 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 versions 11.0 – 11.5

The following new reporting features are available in version 11.x:

- 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 versions 11.0 – 11.5" on page 24.

New language support in versions 11.0 – 11.5

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 product documentation features in versions 11.0 – 11.5

For product documentation, the following new features are available in version 11.x:

- 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.

Chapter 3

Fixed issues

This chapter includes the following topics:

Fixed in version 11.6

This section lists issues fixed in version 11.6.

Discover issues fixed in 11.6

Table 3-1 Discover issues fixed in 11.6

Issue	Description
2016814	You cannot use Smart Response manual quarantine to quarantine a file from a DFS file share to a non-DFS file share. However, you can quarantine files from non-DFS file shares to DFS file shares.

Endpoint issues fixed in 11.6

Table 3-2 Endpoint issues fixed in 11.6

Issue ID	Description
2354445	Workstations with Windows 7 experience delays when files are copied between the workstation and a NetApp file server.
2573597	Citrix systems experience an increase in system IOPS after a DLP Agent is installed, which causes a degradation in performance.
2629692	The DLP Agent can be uninstalled without entering a password on workstations with Windows 7 by executing `AgentInstall.msi`.
2667572	Microsoft Outlook stops responding when an email is sent to a large recipient list.
2693872	Inline graphics that reside in the body of a Lotus Notes email cannot be detected.
2730214	Lotus Notes experiences delays and excessive server polling when an email is sent.
2730219	Microsoft Outlook 2010 stops responding when encrypted or signed emails are sent.
2731896	Data Loss Prevention notification messages are not displayed when a Windows 7 workstation is used to send a Lotus Notes email that violates a policy.
2750364	Network performance is affected when workstations with DLP Agents query Active Directory for a Data Loss Prevention policy that does not contain any Active Directory group conditions.
2771200	Microsoft Outlook stops responding when an email is sent to a large local-distribution list.

Enforce Server issues fixed in 11.6

Table 3-3 Enforce Server fixed issues in 11.6

Issue ID	Description
2647623	When configuring protocol filtering for a Network Monitor Server: Selecting Use Custom Settings and adding a custom protocol after you have edited the built-in protocols at the System > Servers > Overview > Configure Server page causes an “unexpected error” to occur; you will not be able to apply your custom settings to a specific server in this situation.

Mobile Prevent issues fixed in 11.6

Table 3-4 Mobile issues fixed in 11.6

Issue ID	Description
2614694	The Pandora iPad app fails to connect to the Pandora server and generates the following error message: "Cannot Connect to Pandora" when traffic is routed through the Blue Coat proxy server .

Network Prevent issues fixed in 11.6

Table 3-5 Network issues fixed in 11.6

Issue ID	Description
1834667	Yahoo Mail posts performed through Firefox may go undetected by Network Prevent. Incorrect Content-Type header (for example, application/x-www-form-urlencoded) is noticed when the email body has XML content. Best effort parsing will be done for these requests and, dependent on parsing output, some violations may go undetected.

Internationalization and localization issues fixed in 11.6

Table 3-6 Mobile internationalization and localization issues fixed 11.6

Issue ID	Description
2582425	Non-ASCII data in the body and subject of an email may not get inspected when sent to Gmail through the iOS Safari Web browser. Symantec Data Loss Prevention for Mobile cannot detect the encoding mechanism that is used by Safari.

Fixed in version 11.5.1

This section lists issues fixed in version 11.5.1. Most of these issues are fixes on the Symantec Data Loss Prevention server side. One Detection issue (2620720) is fixed on both the endpoint agent and server side. One Endpoint issue (2674393) is fixed on the endpoint agent side.

Detection issues fixed in 11.5.1

Table 3-7 Detection issues fixed in 11.5.1

Issue ID	Description
2620720	The previous version of iDefense had KeyView filter overflow vulnerabilities with bitmap (.bmp), OpenDocument (.odp), and Freelance Graphics (.pre) files. This is both an endpoint agent and server-side fix.
2656323	Symantec Data Loss Prevention was unable to trigger incidents on protected Microsoft Excel workbooks. This is a server-side fix.
2673892	Due to an error ("com.vontu.cracker.CrackingException: Failed to obtain the content extractor reference"), Symantec Data Loss Prevention did not properly delete temporary files (kpXX.tmp), causing excess use of disk space. This is a server-side fix.
2673910	Symantec Data Loss Prevention was unable to trigger incidents on Microsoft Project files. This is a server-side fix.

Discover issues fixed in 11.5.1

Table 3-8 Discover issues fixed in 11.5.1

Issue ID	Description
2674369	Due to an issue in the Microsoft netuse caching mechanism, the File System crawler threw many erroneous "Multiple Connections to the same server not allowed" errors. This is a server-side fix.
2674373	The Symantec SharePoint solution could not limit a scan to the site collections under a specified web application URL. This is a server-side fix.
2681930	Symantec Data Loss Prevention did not support SSL certificates with wildcards. This is a server-side fix.

Documentation issues fixed in 11.5.1

Table 3-9 Documentation issues fixed in 11.5.1

Issue ID	Description
2648478	The variables in the online Help for configuring BoxMonitor.Channels were translated in localized versions of Symantec Data Loss Prevention.

Endpoint issues fixed in 11.5.1

Table 3-10 Endpoint issues fixed in 11.5.1

Issue ID	Description
2674392	Symantec Data Loss Prevention did not clean up old .tmp files when exceptions were thrown during incident processing. This is a server-side fix.
2674393	Symantec Data Loss Prevention did not truncate large files correctly when data retention was on, causing incident processing to fail on the Endpoint Server . This is an endpoint agent-side fix.

Enforce Server issues fixed in 11.5.1

Table 3-11 Enforce Server issues fixed in 11.5.1

Issue ID	Description
2673983	Symantec Data Loss Prevention quit unexpectedly when sending a report with a custom attribute as a filter. This is a server-side fix.
2673975	Symantec Data Loss Prevention quit unexpectedly when saving custom protocol settings at the server level. This is a server-side fix.
2673994	CSV exports of incidents that included the User Cancel response rule were formatted incorrectly. This is a server-side fix.

Network issues fixed in 11.5.1

Table 3-12 Network issues fixed in 11.5.1

Issue ID	Description
2674398	The Network Monitor did not detect Hotmail streams. This is a server-side fix.

Upgrader issues fixed in 11.5.1

Table 3-13 Upgrader issues fixed in 11.5.1

Issue ID	Description
2697179	The Symantec Data Loss Prevention 11.5 Upgrader did not upgrade three JAR files required for crawling SharePoint data sources. Symantec Data Loss Prevention could not scan any SharePoint data sources. This is a server-side fix.

Fixed in version 11.5

This section lists issues fixed in version 11.5.

Detection issues fixed in 11.5

Table 3-14 Detection issues fixed in 11.5

Issue ID	Description
2290331	IDM matching of large binary files was not working due to an Advanced Setting.

Fixed in version 11.1.2

This section lists issues fixed in version 11.1.2.

Detection issues fixed in 11.1.2

Table 3-15 Detection issues fixed in 11.1.2

Issue ID	Description
2586641	A crash of the default content extraction plug-in results in an operating system pop-up dialog notification that must be dismissed interactively. This results in the stoppage of any Endpoint Discover repository scan than may be in progress.
2590894	Frequent default content extraction plug-in crashes result in excessive File Reader restarts and no incidents being generated.
2559436	Detection server cannot perform content extraction on DIF and JTD file types.
2297493	Compilation error for custom file type script may cause the script engine to crash.
2497782	Recipient rule exceptions with multiple email addresses result in match highlighting errors for SMTP endpoint incidents.
2421018	After the Content Extraction Host (CEH) restarts, nested subfiles may not be extracted.
2571271, 2571273	Log facility enhancements for Content Extraction Host and API.
2519549	A failure with content Extraction during a Network Discover scan results in a null pointer exception due to the content not being available.

Discover issues fixed in 11.1.2

Table 3-16 Discover issues fixed in 11.1.2

Issue ID	Description
2559524	Out of memory error while mounting a share causes the Discover Server to run out of drives to mount on.

Documentation issues fixed in 11.1.2

Table 3-17 Documentation issues fixed in 11.1.2

Issue ID	Description
2563516	Oracle Guide update: Add missing step that you need to copy the contents of ZIP 2 of Oracle 32 download into folder of ZIP 1.
2588117	Upgrade Guide update: Add details about Data Identifiers, importing from v10 to v11.
2586614	Administration Guide update: Fix info about kinit (not available as part of the Data Loss Prevention download).
2408872	Administration Guide update: More description for Logging.OperationLogTTL.int in Table 9-11.
235444	Administration Guide update: "Internet Explorer" should be "Windows Explorer" for description of Hooking.EXPLORER_HOOKING.int advanced setting.
2596611	Administration Guide update: Corrected info about language pack platform support (Guide had said that language packs were only available for Windows).

Endpoint issues fixed in 11.1.2

Table 3-18 Endpoint issues fixed in 11.1.2

Issue ID	Description
2417186	Minimized the occurrence of an error message on copying data from PDF to the clipboard.
2530338	Performance enhancements to the Agent Overview page.
2564697	Upgrade to v11.1.1 fails if the product was installed using UninstallPassword Key.
2425220	Microsoft Explorer crashes on simultaneous folder copy operation.
2534627	Invalid pointer access can cause the DLP Agent to crash during shutdown.

Enforce Server issues fixed in 11.1.2

Table 3-19 Enforce Server issues fixed 11.1.2

Issue ID	Description
2406883	Unable to select multiple user groups at the user groups management screen.
2531372	Unable to set a minimum ignore size for monitoring Web prevent messages.
2427987	Unable to remove a detection server if the name of the server exceeds the maximum allowed characters for server names.
2412247	Error appears when trying to open the Folder risk report page on an upgraded system.
2443377, 1998097, 1493713	No warning is displayed when using an unsupported browser.
2524447	Unable to view more than 20 rows of the second level in a double Incident Summary report.
2415084	Group-based policy with a configured user group appears to import properly, but the imported policy does not detect any incidents based on the user group configuration.
2513303	Policy export does not import detection rule exceptions correctly.
2488108	Syslog messages have an improperly formatted header.
2534101	Computer IP address is missing from the Reporting API incident details for Endpoint incidents.
2395301	User interface fix related to Symantec Data Classification Service.
2430204	Unable to export summarized report as CSV.

Installer and Upgrader issues fixed in 11.1.2

Table 3-20 Installer and Upgrader issues fixed 11.1.2

Issue ID	Description
2406144	Java upgrade for security updates.
2427991	Upgrader prompts user for certificate even if browser has certificates installed.

Network issues fixed in 11.1.2

Table 3-21 Network issues fixed 11.1.2

Issue ID	Description
2424589	When processing email messages with multiple recipients, the buffer overflow is reached and produces the error message “Buffer too big for SSL encryption.”

Fixed in version 11.1.1

This section lists issues fixed in version 11.1.1.

Classification issues fixed in 11.1.1

Table 3-22 Classification issues fixed 11.1.1

Issue ID	Description
2250824, 2302168	Certain plain text files fail to be classified properly due to the existence of certain words which are also SMTP commands. The detection engine believes that these files are not plain text.
2093053	Negative timeout value exceptions may be observed due to Jetty defect.
2339602	For Data Classification Services, the Enforce console does not display all users in a large distribution list (over 1500 users).

Detection issues fixed in 11.1.1

Table 3-23 Detection issues fixed 11.1.1

Issue ID	Description
2366935	An issue with Autonomy causes multiple overflows.
2381488	During detection, if a message causes an out of process IDM policy to run out of memory, subsequent messages will not be detected until the file reader is restarted.
2344889	The Data Identifier for HKID is not matching valid identifications.
2399447	An Autonomy KeyView vulnerability for IBM_CERT.
2123605	Files containing large amounts of metadata may cause a crash in the content extraction API module during unmarshalling.

Table 3-23 Detection issues fixed 11.1.1 *(continued)*

Issue ID	Description
2378975, 2390251	Content extraction fails to recover from certain situations, causing messages to not be processed.
2368512	Plug-ins that write to stdout will cause a filereader crash/restart.
2308820	Subfile extraction does not work for custom content extraction plug-ins.
2318878	VML context-sensitive help is not displayed from Profile Details page.
2354575	The Message ID cache uses excessive backing storage memory.

Discover issues fixed in 11.1.1

Table 3-24 Discover issues fixed 11.1.1

Issue ID	Description
2350446	A Discover scan terminates if an exception occurs while opening the SharePoint root folder.

Endpoint issues fixed in 11.1.1

Table 3-25 Endpoint issues fixed 11.1.1

Issue ID	Description
2291543	The Endpoint Server resends unnecessary data to Symantec DLP agent when the agent reconnects to the server.
2342376	Your web application hangs when printing PDFs from within Internet Explorer.
2366155	Continuously restarting the Symantec DLP Agent as a result of a driver failure can cause the Active Directory server to become non-responsive.
2366158	When the Symantec DLP Agent restarts because of a driver error, an incorrect status can be displayed in the event viewer. You may see the following error: “The EDPA service terminated with the following error: You were not connected because a duplicate name exists on the network. Go to System in Control Panel to change the computer name and try again.”
2399428	The EDPA service crashes if a version 10.5.3 agent is connected to a version 11.0 Endpoint Server.
2274398	The EDPA service may not start after upgrading an agent from 9.0.3 to 11.1.
2374979	Removable media metadata-based policies do not recognize encrypted devices.

Table 3-25 Endpoint issues fixed 11.1.1 *(continued)*

Issue ID	Description
2387163	The Symantec DLP Agent cannot interact with Lotus Notes 6.x multi-user installations.

Enforce Server issues fixed in 11.1.1

Table 3-26 Enforce Server issues fixed 11.1.1

Issue ID	Description
2396049	MonitorController can take a long time to start and may show an out of memory exception in the log.
2402020	The System Overview function may run out of memory if large numbers of Detection Servers combined with large numbers of Policy Groups.
2402021	Monitor Controller ModelCLOBReader errors prevent objects from being distributed to Detection Servers.
2390361	Network Monitor Controller can experience errors sending data to Detection servers when the data is based on a Model object containing a LOB and the LOB locator is no longer valid.
2395222	The System Overview page may run out of memory if large numbers of Detection Servers are combined with large numbers of Policy Groups.
2350426	Files containing large amounts of metadata may cause a crash in the Enforce Server in the content extraction API module during unmarshalling.
2367005	Security vulnerability with Remote exploitation of a stack buffer overflow in the Autonomy KeyView SDK.
2400535	Any Server FlexResponse plug-ins that write to stdout cause the filereader to crash or restart.
2297558	Product Integration Status on the SPC Home page is not updated after registering a detection server.
2380116	System Alert emails are not sent when scheduled in the Enforce Server.
2374156	Match highlighting context length is now configurable in Manager.properties.
2410311	Scheduled reports of dashboards cannot be sent through email.
2293177	Directory Group rules are being dropped when the Policy matrix is sent to v10 agents. This means that Policies that use Sender Directory Group rules will never match on an older agent
2210688	When you configure a user group on the Enforce Server with a nested security group/distribution list added to the groups list, the email sent for classification does not trigger policies created with sender/recipient user group rule.

Table 3-26 Enforce Server issues fixed 11.1.1 *(continued)*

Issue ID	Description
2310384	The Policy menu may throw an exception if the v11.0 Enforce Server was upgraded on a 64-bit system.
2338387	Enforce Server throws an exception when creating a new user with password rotation enabled.
2393327	The new bulk incident deleter is not enabled by default.
2399414	The MonitorController service takes a lengthy time to start and occasionally runs out of memory.
1720370	In an emailed report in Microsoft Outlook 2003, the applied filters section is overlapped by the section that follows.
2371154	User group editing page submits group values as a GET which can limit size or characters supported

Installer and Upgrader issues fixed in 11.1.1

Table 3-27 Installer and Upgrader issues fixed in 11.1.1

Issue ID	Description
2366161	Endpoint Drivers are not verified to be present after installation completes.
2320284	Performance of the 11.0 Upgrader degrades when a large number of endpoint incidents are present.
2276890	The Windows upgrader uses an absolute path to locate the 32-bit version of xcopy, and will fail on all detection servers if that binary is in a nonstandard location.
2320270	The Symantec Data Loss Prevention Endpoint upgrade may fail if any of the following applications are specified to be monitored by the Symantec DLP Agent: ■ Microsoft Live Meeting Client 7 ■ Microsoft Live Meeting Client 8 ■ WebEx Communication Module ■ Microsoft Office Communicator ■ Microsoft Windows Bluetooth ■ Google Talk ■ Apple iTunes
2320271	The Symantec Data Loss Prevention upgrade may fail if the combined length of EndpointFilePath and EndpointFileName is longer than 255 characters.

Network issues fixed in 11.1.1

Table 3-28 Network issues fixed 11.1.1

Issue ID	Description
2310000	Network Monitor servers are getting incorrect configurations (protocols and filters). Network traffic is not being processed as configured in the administration console.
2318661	Network Monitor fails to process corresponding traffic defined in customer IP Filter in SMTP on Linux32 for fresh installations.
2317533	For non-FIPS mode, STARTTLS handshake doesn't support SSLv3 and SSLv2.
2349595	Sender/Recipient domain rules due to a change in L7 with how the Network Server parses email addresses of the form: “lastname, firstname” <myemail@domain.com
2355391	Certain Web applications can hang when printing PDFs from Internet Explorer.

Fixed in version 11.1

This section lists the known issues fixed in version 11.1.

Classification issues fixed in 11.1

Table 3-29 Classification issues fixed 11.1

Issue ID	Description
2122262	Exchange messages that are delivered from a Classification Server do not include Envelope information. Because the Subject of a message is part of the mail Envelope, a detection rule that examines only the Envelope component will never detect content in Subject line of these Exchange messages

Detection issues fixed in 11.1

Table 3-30 Detection issues fixed 11.1

Issue ID	Description
2177541	The ContentExtraction.MaxContentSize Advanced Server Setting does not apply to the text file type (*.txt) for the affected server.

Documentation issues fixed in 11.1

Table 3-31 Documentation issues fixed 11.1

Issue ID	Description
2347857	The *Upgrade Guide* incorrectly indicates that an upgrade from version 10.x directly to v11.1 is possible. The latest version of the Upgrade Guide contains the correct information. You can get the latest version of the guide on FileConnect.
2327853	The*Upgrade Guide* “What’s New” section states that Microsoft Windows 2008 32-bit and 64-bit R2 is supported for the entire Symantec Data Loss Prevention system. This is incorrect. Microsoft Windows 2008 64-bit R2 Enterprise Edition is only supported for Symantec DLP Agents. Microsoft Windows 2008 32-bit Edition is not supported.
2341897	Under the section “Launching the Upgrade Wizard on the Enforce Server”, in both the Linux and Microsoft Windows versions of the *Upgrade Guide*, the name of the file in Step 5 is incorrect. The correct name of the file is: `11.1_Upgrader_Windows.jar`.
2342116	Under the section “Importing SSL certificates to Enforce or Discover servers”, in the *Administration Guide*, the keytool command in Step 3 is incorrect. The correct command is: `keytool -importcert -alias new_endpointgroup_alias -keystore ..\lib\security\cacerts -file my-domaincontroller.crt` In this example command, `new_endpointgroup_alias` is a new alias to assign to the imported certificate and `my-domaincontroller.crt` is the path to your certificate. Additionally, the command in Step 4 of the same procedure is incorrect. The correct command is: `keytool -importcert -alias new_endpointgroup_alias -keystore ..\lib\security\cacerts`
2179160	When defining a data identifier pattern, the regular expression “\w” does not detect the underscore (_) character. Note that this defect only applies to the Content Matches Data Identifier detection method, not to the Content Matches Regular Expression detection method. Refer to the topic "About pattern language limitations for data identifiers" in the *Symantec Data Loss Prevention Administration Guide* and in the online Help.

Endpoint issues fixed in 11.1

Table 3-32 Endpoint issues fixed 11.1

Issue ID	Description
2245552	If an Endpoint FlexResponse plug-in uses code to create a file that contains sensitive data, any USB copy event that triggers the plug-in results in multiple copies of the file, and multiple incidents logged to the Enforce Server administration console.
1944319	CD/DVD monitoring cannot be disabled on Windows 7 and Vista for Windows CD/DVD burning software. This issue only affects Windows 7 and Vista operating systems.
1949060	Disabling the Removable Storage option from the endpoint server configuration does not affect Citrix Volume monitoring. The Symantec DLP Agent continues to monitor Citrix Volumes irrespective of this setting.
2093077	The Rules Results Cache (RRC) stores results for previously seen files. If a data identifier definition is changed this cache does not get cleared and may hold results for old data identifier rules which may not be valid anymore.
2146393	The File Size Ignore filter is not supported for any USB removable drives on Citrix XenApp clients.
2166471	Any changes made to detection advanced settings do not take effect if rule results caching (RRC) is enabled. The RRC cache is not cleared.
2167995	The Symantec DLP Agent remembers the position of the last connected Endpoint Server from the list of available Endpoint Servers. After running the Change Endpoint Server task, the agent tries to connect to whichever server is in the same position from the new Endpoint Server list.
2240376	The 32-bit Symantec DLP Agent was released with unsigned driver files. When you install the 32-bit Symantec DLP Agent on an endpoint computer that restricts unsigned applications, the operating system displays warnings about installing unsigned drivers.
2245088	If an Endpoint FlexResponse action attempts to invoke a create, copy, or save a sensitive file, that action is triggered multiple times. On the Enforce Server administration console, these multiple actions show up as numerous incidents that are created from a single event. This issue occurs on Microsoft Windows Vista or Microsoft Windows 7 endpoint computers when local hard drive monitoring is enabled.

Table 3-32 Endpoint issues fixed 11.1 *(continued)*

Issue ID	Description
2146932	The Symantec DLP Agent does not monitor newer Microsoft Office file types such as *.docx or *.pptx when the file type filter configuration is not set to monitor *.zip files and the default action is set to Ignore. The agent identifies these newer Microsoft Office files as a *.zip archive file. However, if the detection file type configuration is set to monitor file types other than *.zip and also set with a default action of Ignore, then the Microsoft Office files are ignored along with all other files that contain a *.zip signature.

Enforce Server issues fixed in 11.1

Table 3-33 Enforce Server issues fixed 11.1

Issue ID	Description
2164917	The Enforce Server allows a “:” in the name of a detection server. Detection servers cannot contain the “:” symbol. Detection servers containing this symbol experience issues when starting up.
2148495	Monitor Controller service does not restart automatically after a system restart.
2047291	The sslkeytool utility does not run correctly on FIPS-enabled Enforce Servers.
2168915	Editing the same user group from multiple Enforce Server sessions at the same time results in an fatal error.

Internationalization and localization issues fixed in 11.1

Table 3-34 Detection internationalization and localization issues fixed 11.1

Issue ID	Description
1677667	When processing a file whose name contains certain asian characters on Japanese endpoints, the file cannot be opened. No incidents will be generated for the file.

Table 3-35 Enforce Server internationalization and localization issues fixed 11.1

Issue ID	Description
2152196	The following error message appears if you save reports with non-ASCII characters in the report names: “Report name is not unique”.

Table 3-35 Enforce Server internationalization and localization issues fixed 11.1 *(continued)*

Issue ID	Description
2164917	The Enforce Server allows a ":" in the name of a detection server. Detection servers cannot contain the ":" symbol. Detection servers containing this symbol experience issues when starting up.

Chapter 4

Known issues

This chapter includes the following topics:

- Known product issues
- Known internationalization and localization issues

Known product issues

The following tables list known issues by product module. The issue ID is an internal number for reference purposes only.

Classification known issues

Table 4-1 Classification known issues

Issue ID	Description	Workaround
2102965	If you restart a Classification Server, the System Overview screen (System > Servers > Overview) may show more incidents for that server than are actually stored in the Enforce Server database. This occurs when Classification policies enable Classification Test Mode and specify a maximum threshold for the number of stored Test Mode incidents. After the server restarts, the incident total for the server can increase up to the sum of the threshold amounts, even though no new incidents are added to the Enforce Server database.	None.
2125667	Classification policies cannot detect the user name or email address for an Exchange message that is sent “On behalf of” another user. When a user sends an Exchange message “On behalf of” another user, Classification policies detect on the user name and/or email address for the user sending the message.	None.

Table 4-1 Classification known issues *(continued)*

Issue ID	Description	Workaround
2193796	Symantec Data Loss Prevention cannot classify an email message based on the IP address of the Exchange server which is part of the header information of the mail item. However, Symantec Data Loss Prevention can classify messages based on the domain name of the Exchange server.	None.
2185534	The Classification Server always treats attached Microsoft Exchange items (such as other email messages, tasks, calendar invitations, and archived email) as part of the body of the email message. If you create a detection rule that inspects only message attachments, the rule will not match content that is present in attached Microsoft Exchange items.	When you create a policy to classify Microsoft Exchange messages, select the Body component as well the Attachments component to inspect Microsoft Exchange items that are attached to email messages.
2259428	File-size filters are broken on new installations. The file size filters “Greater than”, “Less than”, and “Is between” do not appear correctly for Classification incidents on fresh installation setups.	None.
2281475	The Data_Classification_Enterprise_Vault_v11.1.vsp file creates a policy group named Data_Classification_EV_v11.0.	None.
2323325	When importing the Enterprise Vault Solution Pack, an error pop-up window appears that indicates that the solution pack is previous version than the installed version of the Data Loss Prevention solution.	Click Yes to close the pop-up window and then install the solution pack. This is expected behavior. The solution pack version is correct.

Detection known issues

Table 4-2 Detection known issues

Issue ID	Description	Workaround
1799071	If multiple recipients are specified in the Recipient Pattern field and the MatchCounting option is greater than 1, incidents are not created even if two or more recipients match the pattern. Incidents are not created either on the detection server or stored in the Symantec DLP Agent.	When creating the Recipient Pattern rule, set MatchCounting to “At least 1 recipient must match.”
1826457	DGM policies based on EDM profiles do not detect email addresses formatted in Lotus Notes hierarchical format.	None.

Table 4-2 Detection known issues *(continued)*

Issue ID	Description	Workaround
1851220	Endpoint Email/SMTP cross-component matching of compound EDM or IDM policies does not work when the keyword or regular expression pattern is in the Subject line and the EDM/IDM violation is in the Attachment. For example, a policy contains a compound rule with a keyword and IDM condition. If a message is sent with a keyword violation in the subject line and an IDM violation in the attachment, Endpoint Prevent will not register this incident.	None.
1852542	False positive incidents may be generated with a compound exception where one rule is a Context type exception and the second is a DCM exception.	After compounding the DCM exception to a Context type exception, change the default selection from "Matched Components" to "Entire Message."
1974742	A policy that specifies a different Severity level based upon the number of incident matches may generate an Endpoint incident with an incorrect Severity level. For example, a policy is created with the following Severity settings: ■ Default Severity = Info. ■ Severity = High, if (# of matches) > = 20. ■ Severity = Medium, if 10 < (# of matches) <20. ■ Severity = Low, if (# of matches) < = 10. The resulting incidents do not contain Severity levels that match the Severity settings.	None.
1998804	For VML, the size of small training files (less than 1 KB) may be reported as zero in the profile	Ignore the incorrect file size that appears in the Enforce Server administration console.
2086670	For a VML profile, when you adjust the Similarity Threshold, the Enforce Server re-syncs the entire profile with the Detection Servers and Symantec DLP Agents. If you have a large VML profile and possible bandwidth limitations (for example, many endpoints per detection server), this may cause network congestion.	Create the VML profile and accept the default Similarity Threshold. Perform testing to determine the optimal threshold and adjust it to that level. (See the *Vector Machine Learning Best Practices Guide* for testing and tuning guidance, which is available at the DLP Knowledgebase.)

Table 4-2 Detection known issues *(continued)*

Issue ID	Description	Workaround
2111850	All available VML profiles are transferred to every detection server and Symantec DLP Agent even if those profiles are not required by the active policies on that server or endpoint computer. Detection servers load all VML profiles into memory regardless of whether or not any associated VML policies are deployed to those servers. Over time, this reduces server performance. However, Symantec DLP Agents only load the VML profiles that are required by an active policy.	Do not create unnecessary VML profiles. Remove any VML profiles that are not required by active policies.
2121191	If you use Microsoft Outlook 2003 or 2007, Symantec Data Loss Prevention cannot detect data from a chart you insert in the message by performing Insert > Chart. However, Symantec Data Loss Prevention can detect data from an Excel chart you embed in the message as an object (Insert > Object > Excel Chart).	To detect the content of inserted charts in Outlook messages, write a plug-in using the Content Extraction SPI. Refer to the *Symantec Data Loss Prevention Content Extraction Plugin Developers Guide*.
2129686	You cannot import v10.x policies containing Data Identifier or Keyword Matching rules or exceptions to the v11.x Enforce Server.	See the topic “Importing v10 DI and Keyword policies to v11.x systems” in the *Symantec Data Loss Prevention System Administration Guide*.
2131156	You cannot detect custom file types on the endpoint if you combine a Custom File Type Signature condition with an EDM condition in the same policy rule.	Use a Data Identifier condition with a Custom File Type Signature condition to detect precise data from custom file types on the endpoint.
2191684	Keyword Proximity matches are counted per matched pair on a detection server. However, they are counted per word on an endpoint computer. Policies set to create incidents above a match threshold can produce inconsistent results between the products.	Do not use match thresholds with Keyword Proximity conditions.
2203882	When configuring a detection condition for Classification to match on only the body of an email message, Classification policies match on the body of the email as well as the body of all emails attached to it even if they are email attachments of email attachments. Any attachment that is not an email itself, will not match. Additionally, when configuring a detection condition for Classification to match on only attachments, Classification policies match on all attachments with the exception of the body of emails attached; all other attachment types will match even if they are part of attached emails.	None.

Table 4-2 Detection known issues *(continued)*

Issue ID	Description	Workaround
2244571	Configuring policies with Endpoint detection rules and non-Endpoint response rules, such as a Network-Prevent response rule, can cause the detection server to become unstable.	Configure policies that contain Endpoint detection rules only with Endpoint response rules.
2711768	If you configure a keyword condition in a policy and match on the "Subject" only, the detection engine may fail to generate incidents if the message contains a MIME encoded-word subject line.	Use "Envelope" (header) in the match on selection when defining the keyword condition.

Discover known issues

Table 4-3 Discover known issues

Issue ID	Description	Workaround
2529816, 2531206	Some items on broadcast sites created with Microsoft Web Apps on SharePoint 2010 servers are not scanned. Only the following items on broadcast sites are scanned: Announcements, Calendar items, Tasks, and Shared Documents.	None.
1961596	Network Protect (copy or quarantine) does not work on Windows 2008 DFS file shares. Network Protect works on Windows 2003 DFS file shares.	None.
1974658	For a Discover integrated Exchange 2007 target, the “open in browser” link in the Discover incident snapshot does not open the correct document.	None.
2070201	For the integrated Exchange Discover target, the mailbox name in “Specify User Mailboxes to include in this Target” does not allow some special characters in the name. Only alphanumeric characters and the following special characters are allowed in mailbox names: ! # $ ' - ^ _ ' { }.	None.
2073171	From the Folder Risk Report, clicking on links to other reports (such as Incident Lists, Incident Summaries, and Data Insight console reports) triggers a pop-up blocker in Microsoft Internet Explorer 8.	When the Internet Explorer 8 pop-up blocker displays a warning near the top of the browser window, click on the warning and choose to always allow pop-ups from the Enforce Server.

Table 4-3 Discover known issues *(continued)*

Issue ID	Description	Workaround
2075096	The Discover report filter "Does Not Match Exactly" is sensitive to path separators. Using "/" when the path separator in the incident contains "\" or vice versa does not produce the expected result.	Use the exact path separator as specified in the content root used to scan the share.
2122460	If a file share has incremental scanning enabled, and you quarantined an entire folder and its contents from the file share, then restore the entire folder from quarantine, the sensitive data in the restored folder will not be scanned again if incremental mode is enabled.	None.
2132915	Starting a scan on a new Discover Server can result in files being re-scanned. This is likely due to the time it takes to propagate the incremental index. If the scan starts before the server has received all of the index updates, then some files can be re-scanned.	Wait a few moments before starting the second scan. Give the index time to update.
2138956	Protect copy remediation fails if blank credentials are used to scan a content root in a Discover target.	Create a separate target for the content root with the blank credentials. Set the default user credentials to blank for that target. Look for the following error message in the `FileReader.log` log file: jcifs.smb.SmbAuthException: The referenced account is currently locked out and may not be logged on to
2150273	In a Discover snapshot of an incident from the integrated Exchange scan, the "Open in browser" option may not work for some items, depending on the item as well as the browser.	Use Internet Explorer if the link fails to work from Firefox and vice versa.
2155333	In Internet Explorer 8, the sender and recipient information is not displayed in Discover incident snapshots from the Exchange server target.	None.
2165549	Custom Data Identifiers created before version 11.0 are not valid after you upgrade to version 11.x. Incidents that were generated from those identifiers will remain, but the Custom Data Identifier name no longer appears in the incident snapshot.	None.
2233064	Libraries for Endpoint FlexResponse and Server FlexResponse are unintentionally available to plug-in developers. Plug-in developers should not see these libraries.	None.

Table 4-3 Discover known issues *(continued)*

Issue ID	Description	Workaround
2240919	A Server FlexResponse plug-in running in multiple threads may leave incidents in the "Requested" protect state.	Limit the number of simultaneous plug-in threads. Set the default number in the maximum-thread-count property in the plug-in properties file to 1.
2703756, 2737410, 2738374	The **Scan History** page always displays the incident count of Endpoint Discover scan targets as **N/A**.	To view the incident count for an Endpoint Discover scan target, go to the **Scan Details** page by clicking the link in the **Scan Status** column.
2725480	The **Discover Targets** page no longer displays the Scheduled Pause or Resume date and time of Discover target scans.	None.
2721065	If you are using Microsoft Internet Explorer version 8 or 9, error messages displayed on the **Discover Target** page disappear immediately.	There are two workarounds for this issue: ■ Apply the Cumulative Security Update for Microsoft Internet Explorer: http://technet.microsoft.com/en-us/security/bulletin/ms12-010 ■ Use Mozilla Firefox.

Endpoint known issues

Table 4-4 Endpoint known issues

Issue ID	Description	Workaround
1665980	Occasionally, the Symantec DLP Agent uninstaller does not remove all of the files from the previous version of the Symantec DLP Agent from your system. This happens if a previous installation process failed and the reference count of the installed files is not reset to 1.	You must manually delete any files that have not been deleted.
1737520	When Microsoft Outlook is running and the otlrdm.dll is loaded into it, the Symantec DLP Agent installer cannot delete the otlrdm.dll during uninstallation. A "File in use" warning dialog box is displayed.	Clock the Microsoft Outlook application and click the **Retry** button.

Table 4-4 Endpoint known issues *(continued)*

Issue ID	Description	Workaround
1792941	Agent regular expressions are case sensitive. If the goal is to match upper and lower case data, create an endpoint regular expression policy that contains both upper case and lower cases versions of the regular expression. For example, the following data contains different cases of the initial letter: ■ C0000763012 ■ I0020126407 ■ i0020126407 ■ c0000763012 Although the data contains different cases, it is essentially the same. Endpoint agents regard each case as a separate instance.	Create an endpoint regular expression policy that contains both case-sensitive and case-insensitive versions of the regular expression.
1822354	On the Symantec Management Console, DLP Integration Component (IC) Reports displays all computers associated with your system. DLP Reports ignores all groups and roles. You cannot narrow the report to a subset of computers for your network.	None.
1829171	In rare circumstances, incidents held in the agent can get queued and are not sent to the Endpoint Server in a timely manner. For example, this can happen if the file scan experiences unusually high activity.	Restart the Symantec DLP Agent.
1861123	If there are not any Limit Incident Data retention rules configured for two-tier detection on Endpoint Prevent, attachments containing violating text are dropped.	None.
1902505	If the file extension filter configuration is not correct, if it contains commas or other nonnewline separators, no error message is displayed to indicate this. If the configuration is not correct, the file extension filters will not work. .	Ensure that file extension filters are separated only with new lines, and not with any other characters such as commas, semicolons, or any other punctuation.

Table 4-4 Endpoint known issues *(continued)*

Issue ID	Description	Workaround
1982811	When confidential files are saved using Microsoft Word 2007 and Microsoft Excel 2007 to a local drive, only the temporary file name is reported in the incident. This issue was not consistently reproducible on all systems. The issue was observed with the following applications: ■ Microsoft Word 2007 12.0.6504.5000 SP1 MSO (12.0.6320.5000) ■ Microsoft Excel 2007 12.0.6514.5000 SP1 MSO (12.0.6320.5000)	None.
1986141	If you are using clean_agent.exe for cleaning corrupt agent installations and have Norton Internet Security installed on same endpoint, there is a possibility that Norton will treat clean_agent.exe as a virus and will delete it. .	White-list clean_agent.exe in Norton Internet security application.
2074287	If a Symantec DLP Agent contains some edpa log files with plain text and other edpa log files with obfuscated text, then the resultant log file that is pulled by the Troubleshooting Task, from either DLP IC or the Enforce Server, will contain garbled text. Workaround:	None.
2076523	The Collect Agent Logs task keeps running if agent logs are not present on the Endpoint Server. If no agent logs are available on the Endpoint Server, the Collect Agent Logs task continues to run and cannot stop. Workaround: Cancel the existing Collect Logs task and execute a Pull Logs task from the Agent Overview page so that agent logs are pulled to the Endpoint Server and then run the Collect Logs task again.	None.
2078404	Application Monitoring may not be able to block violating files with Read monitoring if a user double clicks to open the file.	Use file monitoring in Open mode.
2093311	If an application is registered for Application Monitoring and opens a file residing on a network share, it will not be scanned and cannot be blocked if contains sensitive information.	None.
2100592	If the Symantec DLP Agent is stopped during a USB data transfer, Windows Explorer crashes.	None.

Table 4-4 Endpoint known issues *(continued)*

Issue ID	Description	Workaround
2109217	In the DLP IC, there is an error on the Agent Configuration Details report page when you expand the Actions drop-down or when you right-click the Symantec DLP Agent. No actions appear.	If you want to perform actions on your computer resource then Agent Deployment Details reports can be used. All necessary actions, for example, Properties, Move, Delete, and others are accessible through the Agent Deployment Details report in DLP IC.
2112763	If a text editor has been added to Application Monitoring, a block pop-up message can be displayed if you use the text editor to save sensitive information. This pop-up displays when the application monitoring setting for the text editor is set to File Open. Although the pop-up displays and an incident is generated, the sensitive data is saved in the file. This generally occurs when the text editor tries to re-open the file.	None.
2114107, 2134338	If you have multiple response rules in a policy and an IM incident is generated, the Incident History shows the User Notified response rule instead of the Action Blocked response rule. However, the Action Blocked action was taken.	None.
2119984	Citrix published drives cannot be monitored by Application Monitoring. If an application opens a sensitive file from a Citrix published drive, the file is not scanned for sensitive information.	None.
2124582	On a Symantec Management Platform 7.1 64-bit server, the DLP IC solution gets installed without installing PPA. The DLP IC dashboard shows a server error after launching.	Install the latest version of PPA from Symantec Product Listing before installing or launching the DLP IC solution.
2128427	The printer name is not available in the Incident Snapshot for Microsoft Word applications.	None.
2129471	The Symantec DLP Agent is not compatible with Symantec Norton products.	None.
2131164	There is a possibility that some application will retry to attach file blocked by application monitoring. In such circumstances, endpoint computer users will see multiple pop-ups and multiple incidents will be reported.	None.

Table 4-4 Endpoint known issues *(continued)*

Issue ID	Description	Workaround
2135712	The Incident History for FlexResponse response rule does not display correctly if you have a policy which executes both a successful response rule or action and a failed response rule or action. Messages from the successful response rule/action shows up correctly but the failed response rule/action does not show up in the Incident History.	None.
2136466	For a folder transfer through AIM Pro, the incident details may not show the Sender, Recipient, or Application name. This may happen when AIM and AIM Pro co-exist on a Windows 7 operating system.	None.
2138874	When a file is copied from a network share to local hard drive, the pop-up notification appears multiple times (once for each violation) regardless of the “Apply this Justification to subsequent files” option being selected.	None.
2158070	On Windows 7 64-bit computers, de-registering a Symantec DLP Agent using the de-register policy of the DLP IC Solution or using the Agent Management Registration utility, and then re-registering the Symantec DLP Agent through Enforce by setting SMP.AUTO_ENABLE.int = 1 in the Advanced Endpoint Settings does not register the DLP Agent. Any agent task run after this on the endpoint computer will fail with return code -1.	On Windows 7 64-bit computers, registering and de-registering of DLP Agent should be done using the policy of the DLP IC solution or the Agent Management Registration utility only.
2161098	In SMP, endpoint computers with an Agent Deployment Status as “Not Managed” are not displayed on the DLP home page under DLP Agent Deployment status, DLP IC Reports, and Filters (Not Managed Computers). visible on the DLP Portal page, the DLP IC Reports page, or through the “Not managed” filter.	You can view reports of the endpoint computers with a status of “Not Managed” using the “computers with no agent” SMP filter. The “Computers with no agent” SMP Filter is available under the All Reports tab. You can also access the filter by going to: Notification Server Management > Agent > All Windows 2000/XP/2003/Vista/2008/7 Computers with No Agent.
2166809	When a violating file is copied to a virtual hard drive using a command window [cmd (driver)], it is not blocked. This is because the virtual hard drive is considered to be a local drive by the Symantec DLP Agent when you use cmd or Save-As (driver) to copy the file.	None.

Table 4-4 Endpoint known issues *(continued)*

Issue ID	Description	Workaround
2177690	After upgrading the Symantec DLP Agent to the latest version, the agent must re-connect to the Endpoint Server before detection resumes. The upgrade process deletes all stored policy configurations from the Symantec DLP Agent. Once the agent re-connects to the Endpoint Server, the agent downloads the relevant policies.	None.
2233312	SMP servers cannot connect to FIPS-enabled Enforce Servers.	None.
2252365	You cannot upgrade Symantec DLP Agent running on Microsoft Vista Business SP2 computers. The Symantec DLP Agent services do not restart automatically after the upgrade.	Repair the installation after the upgrade is complete.
2252438	Endpoint FlexResponse incidents are not created when a file with sensitive keywords is created in an EFS protected directory (for example, the User Temp directory).	None.
2323379, 2323399, 2379130, 2405893	The Symantec DLP Agent installation does not support Windows Logo driver certification policy.	Disable Windows Logo certification policy before you install the Symantec DLP Agent.
2431327	The Endpoint incident list does not sort by destination.	None.
2629339	When using Titus to classify documents in combination with Symantec Data Loss Prevention metadata detection, certain tags added by Titus cannot be detected. The data is stored by Titus in the XMP metadata for PDF files which is not extracted by Symantec Data Loss Prevention.	None.
2848627	After upgrading to a new version of Symantec Data Loss Prevention, user actions performed on Citrix-system published drives are only monitored through Windows Explorer.	After upgrading to a new version of Symantec Data Loss Prevention, restart the Citrix machines where Symantec Data Loss Prevention is installed. After the Citrix machines have been restarted, Symantec Data Loss Prevention can monitor user actions performed on Citrix-system published drives that occur outside of Windows Explorer.

Enforce Server known issues

Table 4-5 Enforce Server known issues

Issue ID	Description	Workaround
1741533	When the Symantec Data Loss Prevention Product License expires or no valid licenses are present, an Enforce user without System Administration privileges cannot log on. The user will not be able to navigate the administration console. This occurs because the pages the user would normally see have been disabled.	An Enforce user with System Administrator privileges or the Administrator user should log in to the administration console and update the product license field with a valid, current license.
2084579	When the Vontu Manager service is shut down, it will log a message similar to the following: <date><time>- Servlet MessageBrokerServlet threw unload() exception javax.servlet.ServletException: Servlet.destroy() for servlet MessageBrokerServlet threw exception	Ignore this message.
2092995	On Linux systems, when using Data Insight, the time zone offset for file access query databases does not correspond to the Enforce Server local time zone.	Set the default time zone of the Linux JREs by using the TZ environment variable. To do this: 1. Add the following line to `VontuIncidentPersister.conf`: `set.TZ=GMT` 2. Restart the Incident Persister service. 3. Replace GMT with the identifier for the desired time zone. The timezone identifier should match the path of a file under /opt/Vontu/jre/lib/zi. For example, use the identifier “America/New York” for the eastern time zone, which corresponds to the file /opt/Vontu/jre/lib/zi/America/New_York. Repeat these steps for each Symantec DLP service. Changing the default time zone will change the timestamps on the logs and it is a good idea to keep all of the logs in sync.

Table 4-5 Enforce Server known issues *(continued)*

Issue ID	Description	Workaround
2093054	You can create a role that contains "Folder/Resource Reports" privileges but leaves the "View Incidents" option unchecked on the roles page. A user role configured in this way cannot view the folder/resource reports.	Modify the role to have privileges for viewing discover incidents.
2107082	Enterprise Rights Management (ERM) FlexResponse plug-ins fail to execute on FIPS-enabled systems. This is because the encrypted communications mode uses cryptographic settings that are not supported by FIPS.	Use one of the following workarounds: ■ Do not use FIPS mode. ■ Disable Liquid Machines Enterprise Rights Management FlexResponse encrypted communications when in FIPS mode.
2115767	For a keyword proximity rule, the Delete button does not work when accessed through Microsoft Internet Explorer 7. Also, if you click the Also Match button and add the keyword condition, the "Match any Keyword" text area does not accept user input.	Use Mozilla Firefox or Microsoft Internet Explorer 8.
2214699	In the Server Detail page on the Enforce Server, the CPU Usage detail always displays 0%. This level does not reflect the correct CPU usage.	None.
2610462	On the **Create User Groups** page, the scrollbar is missing from the **Directory** tree view control. (Applies only when using Microsoft Internet Explorer version 9.)	Users can click inside the tree view and navigate using the arrow keys.
2639382	Some Endpoint features incorrectly display in the Enforce Server administration console when the deployment has a Symantec Data Loss Prevention for Tablets license and does not have a license for Endpoint functionality.	None.
2199336	Creating secure Directory Connections may fail in FIPS Data Loss Prevention deployments.	Change the domain controller settings to use FIPS-compatible encryption. Please refer to http://support.microsoft.com/kb/811833 for documentation related to Microsoft Windows 2003 server. A similar solution should be available for Microsoft Windows 2008 server.

Table 4-5 Enforce Server known issues *(continued)*

Issue ID	Description	Workaround
2725442	This bug applies to integrations with Symantec Messaging Gateway that use Email Quarantine Connect FlexResponse plug-in. When a user remediates an email incident in the Enforce Server administration console where a single email message violates multiple policies, Symantec Data Loss Prevention creates an incident for each policy violation. However, when a user remediates one of these incidents from the Enforce Server administration console, only the history record of the incident that was remediated is updated. The history of the other incidents that are associated with the violation are not updated. When remediation is initiated from the Symantec Messaging Gateway Control center, all incident histories are correctly updated.	None.

Installer and Upgrader known issues

Table 4-6 Installer and Upgrader known issues

Issue ID	Description	Workaround
1719273	When upgrading, Symantec Endpoint Protection (SEP) shows tamper protection alerts when edpa.exe restarts in the presence of the Symantec Management Agent.	Add edpa.exe and cui.exe to the SEP tamper protection exception list. Use the following steps: 1. Log in to SEPM. 2. Go to Policies. 3. Under view policies click Centralized Exception. 4. Click Add a Centralized Exception Policy. 5. Click Centralized Exceptions. 6. Add Temper Protection Exception. 7. Enter the full path location of edpa.exe. 8. Repeat steps 1–7 to add cui.exe to the Exception List . 9. Save the new policy. 10. Assign the new policy to the client group. **Note:** This workaround is only applicable for managed SEP clients only. Currently, there is no solution for unmanaged SEP clients.
2413702	On the Upgrade Servers screen of the Upgrade Wizard, some FIPS-enabled Windows installations may stop progressing and time out immediately after transmission of the upgrade package to the server.	Workaround: To upgrade the failed detection servers, log in to each failed server and restart the Vontu Monitor and Vontu Update services, then re-select those servers on the Upgrade Servers page and click the Upgrade button again. The second upgrade attempt should be successful.
1834598	When installing on Red Hat 5, password fields in the installer can become disabled. If any other text field in a screen is clicked, the installer stops accepting input into the password fields on that screen.	Click Next and dismiss the error pop-up window if one appears. Or, if no error is given, click Back to return to the screen. The password fields will now accept input. Enter the password information in the screen before clicking on any other fields.

Table 4-6 Installer and Upgrader known issues *(continued)*

Issue ID	Description	Workaround

2148552	There is an error in the RSA BSAFE Crypto-J 4.0 provider that prevents the CA signed certificate chain from being imported.	Immediately before running the import command, modify `\Vontu\jre\lib\security\java.security` to use a non FIPS provider:
		`# security.provider.1=com.rsa.jsafe.provider.JsafeJCE`
		`security.provider.1=com.sun.crypto.provider.SunJCE`
		Perform the certificate imports, then switch the java.security file back to the previous configuration (using `com.rsa.jsafe.provider.JsafeJCE`). At this point, the Manager should run fine with the new tomcat .keystore file generated above.

2792309	After upgrading the Enforce Server , when a user clicks the **Refresh** button the browser may display a Page Not Found error.	Clear the browser cache or re-launch the Enforce Server administration console.
2787474	If a user is created and the user name has a space at the end of the name, the user cannot log in.	Do not create user names with trailing spaces.
2713699	If you add a license for Mobile Prevent for Web to a Symantec Data Loss Prevention deployment where you have configured a lookup plug-in that uses the HTTP, HTTPS, or FTP protocol filtering options, the lookup attributes are not populated when a user clicks the lookup button.	1 Open the Symantec Data Loss Prevention Enforce Server administration console. 2 Navigate to **System** > **Lookup Plugins**. 3 Select the lookup plug-in from the list of plug-ins. 4 Deselect the FTP, HTTP, and HTTPS protocols. 5 Click **Save**. 6 Select the same lookup plug-in from the list of plug-ins. 7 Select the FTP, HTTP, and HTTPs protocols. 8 Click **Save**.

Lookup plug-in known issues

The following table lists the known issues related to lookup plug-ins.

Table 4-7 Lookup plug-in known issues

Issue ID	Description	Workaround
2681842	The CSV Lookup Plug-In does not populate the custom attributes in the **Incident Snapshot** page after the parameter keys in the **Lookup Plugins List Page** are enabled. This issue is limited to Linux environments.	Navigate to the **Lookup Plugins List Page** and click **Reload Plugins**.
2755010	After upgrading a Symantec Data Loss Prevention system that includes a deployed Custom Java Lookup Plug-In to version 11.6, the plug-in may fail to load. This failure occurs if the plug-in JAR files were copied to the `\SymantecDLP\Protect\tomcat\common\lib` directory before the upgrade. This directory does not exist after you have upgraded to Symantec Data Loss Prevention version 11.6.	1. After the upgrade, manually copy any Custom Java Lookup Plug-In JAR files to the `\SymantecDLP\Protect\tomcat\lib` directory. 2. Restart the **Vontu Manager** service.
2832473	Lookup plug-ins do not appear in the administration console of a FIPS-enabled Enforce Server after you have upgraded to Symantec Data Loss Prevention version 11.6.	A workaround for this issue is available in article 55707 at the Data Loss Prevention Knowledgebase, at: https://kb-vontu.altiris.com.
2833520	Script Lookup Plug-Ins do not appear in the Enforce Server administration console after you have upgraded to Symantec Data Loss Prevention version 11.6.	A workaround for this issue is available in article 55706 at the Data Loss Prevention Knowledgebase, at: https://kb-vontu.altiris.com.

Network known issues

Table 4-8 Network known issues

Issue ID	Description	Workaround
1529271, 1529275	Policies that use the Message Attachment or File Name Match detection rule with the Network: Remove HTTP/HTTPS Content response rule, do not work for Yahoo/Hotmail file uploads.	None.
1709758	During the uninstallation of the Symantec ISA web-filter plug-in, the following error is sometimes seen in the event log: `ISA Server failed to load Web Filter DLL C:\Program Files\Microsoft ISA Server\\symc_isa_plugin.dll.`	There are no known side effects at this time. The symc_isa_plugin.dll is removed properly during uninstall. These errors can be ignored.

Table 4-8 Network known issues *(continued)*

Issue ID	Description	Workaround
1887579, 2285574	ISA firewall service WSPSRV.EXE crashes when Symantec Data Loss Prevention ISA plug-in is enabled. This is due to a buffer size limitation. By default, web filters allocate up to 10 MB per thread to potentially stream data to or from Network Prevent and Microsoft ISA, even though the request may not be that large. This is done to prevent memory fragmentation. When ISA experiences extreme load, (several threads spawned) such large memory allocation quickly results in the Microsoft firewall service running out of memory and crashing.	After installing the Symantec Data Loss Prevention Web filter for MS ISA through the Web filter installer, modify the configuration for optimal performance of the MS firewall service. 1. Open your Windows Explorer and go to the ISA install directory. Typically this should be c:\program files\microsoft isa server. 2. Double-click symc_isa_plugin_gui.exe to launch the Symantec Data Loss Prevention web filter configuration interface. 3. Click the Network tab and set the Connection Retries value to 0. By default it is set to 1. 4. Click the Buffer tab and set the Stream buffer size to 64240. 5. Click Apply and wait for confirmation that configuration changes have been updated. Although unlikely, if you need to change the Stream buffer size from 64240, follow one of these guidelines: ■ Set the Stream buffer size to an even multiple of the ethernet frame size (typically 1460 bytes), and ideally less than the TCP send/receive buffer size. See the Network tab for the default value. ■ Set the Stream buffer size to a lower value in a high-load environment. The changes are applied dynamically. You do not need to start the MS ISA firewall service.
1945046	If a role is authorized to view attachments but not authorized to view an original message, users in that role will not be able to view attachments.	None.

Table 4-8 Network known issues *(continued)*

Issue ID	Description	Workaround
2166589	On 64-bit Windows platforms, Network Monitor cannot monitor VLAN traffic for certain network interfaces.	Open the network interface card device properties in Windows. Change the 'Priority & VLAN' property for the card to 'Priority & VLAN Disabled' to enable packet capture for VLAN traffic.
2168816	Double incidents are reported for violations in Yahoo instant messenger (YIM) version 9. If a violation occurs in a conversation on YIM9, the sender and the recipient’s conversations are separated and each side of the conversation is reported as an incident.	None.
2189858	Information displayed in the user interface for attachments (file name/full file path) is not returned by Reporting API for Network incidents (both Network and Endpoint-Network).	None.
2611849	The **Remove HTTP/HTTPS Content** response action (redaction) does not work for ICAP requests that are received from a Websense proxy server.	None.
2689712	Network Monitor cannot scan any messages that are sent with versions of AOL Instant Messenger (AIM) that have encryption enabled.	None. Network Monitor scans AOL instant messages that are sent without encryption.
2714629	Response rules for SMTP email policies do not execute in the order that is defined in the **Response Rules** screen on the Enforce Server. Blocking response rules have a higher priority than non-blocking response rules.	None.
2776516	Email incidents that pass through a Symantec Mail Gateway can be scanned for data loss. The status of an incident is updated after the incident has been remediated using the Enforce console. If the Symantec Mail Gateway administrator remediates the email, there is a delay before the incident status is updated in the Enforce console.	None.

Mobile Prevent known issues

The following table lists the known issues related to Mobile Prevent.

Table 4-9 Mobile Prevent known issues

Issue ID	Description	Workaround
2598269	When the **Ignore Requests without Attachments** option is checked under the ICAP configuration tab, Exchange Active Sync emails do not get inspected.	None.
2622467, 2623830	When user sends a violating email through the native Gmail or Google app or on an iOS mobile device, the email is blocked by Symantec Data Loss Prevention and the app keeps trying to send the mail, which may result in a poor user experience. The Gmail or Google app may not be usable after it is used to send a violating email.	Delete and reinstall the Gmail or Google app on the iOS mobile device.
2623877	Chat messages from the Facebook app on an iOS mobile device are not monitored by Symantec DLP Symantec Data Loss Prevention. Chat messages are sent using the Jabber (XMPP) protocol, which is not sent over ICAP for inspection.	None.
2623896	Symantec Data Loss Prevention for Mobile does not support the following iOS apps: ■ Skype ■ Podcast ■ Hulu Plus	None.
2628239	The iCloud iPad application is not supported.	None.
2710453	The Mobile Prevent license will not work after upgrading to Tablet Prevent.	A new license for Mobile Prevent is required after upgrading from Tablet Prevent.
2713699	Lookup plug-in attributes are not reported for Mobile incidents after an existing Symantec Data Loss Prevention installation is upgraded to include Mobile Prevent for Web.	Deselect and then reselect the protocol filters for Mobile in the lookup plug-in settings. 1. Click **System > Lookup Plugins**. 2. Click the lookup plug-in to edit it. 3. Deselect FTP, HTTP, and HTTPS protocol filters; then, click Save. 4. Click the lookup plug-in to edit it. 5. Select **FTP**, **HTTP**, and **HTTPS** protocol filters; then, click **Save**.

Known internationalization and localization issues

The following tables list the known issues related to internationalization and localization for each product module.

Detection internationalization and localization known issues

Table 4-10 Detection internationalization and localization known issues

Issue ID	Description	Workaround
1791134, 1866769	Detection for PDF files containing Arabic or Hebrew text fails to detect violations.	None.
1791138	Print monitor fails to detect sensitive Arabic data on the Endpoint when printing from applications such as Notepad, Word, and PDF files.	None.
1866765	Print monitor fails to detect sensitive Hebrew data on the Endpoint when printing from Notepad.	None.
1866867, 1866873	Sensitive data in Hebrew email body text and attachments that are encoded as ISO-8859-8-I is not detected. Attachments to ISO-8859-8-I emails are also not correctly detected even if the attachment name and content is in standard ASCII format. These issues are not observed for ISO-8859-8 emails.	None.
1430029, 1479328	In some cases, when viewing the incident snapshot for an attachment with a non-ASCII file name, the file name may be garbled in the UI.	None.
1466323, 1470209, 1470206	Symantec Data Loss Prevention supports the encoding standards defined and supported in Java 6. Due to interpretation differences between various vendors the same encoding (for example, GB2312) will be supported only to the extent of Java 6 support. For a list of supported Java 6 encodings please refer to: http://java.sun.com/javase/6/docs/technotes/guides/intl/encoding.doc.html.	None.

Table 4-10 Detection internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
1519857, 1463737, 1463747, 1524289, 1791119, 1866773	Certain non-ASCII content of scanned Microsoft Outlook Personal Folders (.PST) files may be garbled in the Enforce UI or undetected. Problems such as the following may be observed: ■ Hyperlinks (location and document name) may be garbled. ■ For Windows-1256-encoded email, the body may not be detected. ■ Hebrew body and subject may remain undetected. ■ For UTF8-encoded mail, body and subject may remain undetected, and attachment file names may be garbled.	None.
1654792	Policies with ASCII digits (1234567890) may not match against data containing Arabic-Indic digits such as the numbers used in Egypt, Iran, Pakistan, and parts of India. In Excel files, Arabic-Indic digits are treated as ASCII numbers, and they match only on ASCII numbers (scanning, printing, CD burning) although they are displayed as Arabic-Indic digits. For Word and text files containing Arabic-Indic digits, the Arabic-Indic digits must be specified in the policy.	The policy has to include match rules for both Hindu-Arabic and Western numbers depending on the kind of file. To match Hindu-Arabic numbers in an Excel files, the policy match rule requires Western numbers. To match Hindu-Arabic numbers in Word or text files, the policy match rule requires Hindu-Arabic numbers.
1708526, 1709649, 1860340, 1503970	During EDM detection, a mixed token is not detected during scanning. A mixed token is, for example, when Asian characters and ASCII characters (or characters that are normalized as ASCII characters) are combined. The EDM indexes may also fail to support non-US field validators like phone numbers or ZIP Codes .	None.
1729175	For some incidents the non-ASCII characters in the incident metadata may be garbled in the user interface. This does not affect detection.	None.
1806721, 1829508	Language-specific detection rules may fail to provide the expected results (German sharp-s, Greek sigma, Japanese Yen, Turkish I and others).	Create separate detection rules for each language-specific detection variation you require.

Table 4-10 Detection internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
1806722	Case-insensitive keyword detection matches incorrectly with the Turkish “I” on the server because there are four different versions of “I” in the Turkish language. The special conversion is not covered in the detection engine. ■ Uppercase equivalent of “I” is “I” and not “I”. ■ Lowercase equivalent of “I” is “I” and not “I”.	Create separate case sensitive policies.
1833344, 1823548	Regular expression for Unicode codepoint fails on the endpoint. For example, searching for Unicode character \u6211 fails. Also the java regular expression reference defines the \w class as containing only ASCII word characters. To match non-ASCII letters you must use the Unicode syntax \p{L}. On the endpoint, the situation is roughly inverse. On the endpoint, the \w works for non-ASCII characters but the \p is unsupported.	Use the international character in the regular expression instead of the code point or \w and or \p{L} class respectively.
2268405	When ANSI text files are used for VML, non-ASCII characters are ignored when extracting keywords to the features file after training profile.	Convert ANSI contents to Microsoft Word Document or UTF8 text format.
2305411	VML detection will not work on Chinese, Korean, or Japanese content detection.	None.

Discover internationalization and localization known issues

Table 4-11 Discover internationalization and localization known issues

Issue ID	Description	Workaround
1704203	Scanner installation on non-English environments has issues when the folder being used for installation (from/ to) has multi-byte characters.	Use a folder with non multi-byte ASCII characters when installing the scanners. Symantec recommends that you use the Network Discover Microsoft SharePoint or Exchange server targets instead of the Microsoft Exchange or SharePoint scanners.

Table 4-11 Discover internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
1727476	When connecting to an SQL Server 2005 content root, you will get the error “Unable to create a database connection” when using credentials which use a password that contains HiASCII characters.	Change the password and do not use HiASCII characters.
1763681	An error “The network name cannot be found” appears when trying to scan a Discover target with ß in folder name using JCIFS.	Use a system mounter instead of JCIFS.
1824358	Scanner configuration files do not support Byte Order Mark (BOM) when saved using UTF8 encoding.	Use a third-party tool such as Notepad++ to save the file without BOM.
1923438	For SharePoint 2007 scanners, VontuSharePoint2007Scanner.cfg job names must be composed of ASCII-only characters. When a non-ASCII job name is used, data is not scanned.	Workaround: Do not use non-ASCII characters for job names. Symantec recommends that you use the Network Discover Microsoft SharePoint or Exchange server targets instead of the Microsoft Exchange or SharePoint scanners.

Endpoint internationalization and localization known issues

Table 4-12 Endpoint internationalization and localization known issues

Issue ID	Description	Workaround
2173748	The Symantec Management Platform (SMP) DLP IC context-sensitive online Help does not launch for Traditional Chinese locales. This is due to how help files for Traditional Chinese are deployed by the platform installer. Context-sensitive help topics that are related to Install, Upgrade, and Uninstall of the Symantec DLP Agent do not display.	Access these online Help topics by opening the “Installing Agents using the Symantec Management Platform” topic from the DLP IC Online Help table of contents.

Enforce Server internationalization and localization known issues

Table 4-13 Enforce Server internationalization and localization known issues

Issue ID	Description	Workaround
2167210	Detection monitors fail to start if the target device name contains non-ASCII characters.	Use the following procedure: 1. Open your registry editor and edit: `HKLM/System/CurrentControlSet/Control/Class/{4D36E972-E325-11CE-BFC1-08002BE10318}/0007/` 2. Change the `DriverDesc` value so that it contains only ASCII characters. 3. Restart the detection monitor.

Installer and Upgrader internationalization and localization known issues

Table 4-14 Installer and Upgrader internationalization and localization known issues

Issue ID	Description	Workaround
1805050	Services fail to start when run by system users with their locale set to Turkish.	Switch the Windows regional settings to English (USA) before installing Symantec Data Loss Prevention. Setting the Default User profile to the US locale results in Symantec Data Loss Prevention system user profiles being created with these settings.
1819443	Creating an Oracle database on a Turkish operating system gives a TNS Protocol Adapter error.	Workaround: Deploy the Oracle database to a non-Turkish operating system.

Network internationalization and localization known issues

Table 4-15 Network internationalization and localization known issues

Issue ID	Description	Workaround
1727543, 1727550	When using keyword matching with non-ASCII characters, some keywords may not be matched against content that uses those non-ASCII characters but has encoded them in a manner not supported by the Java 6 runtime. The problem occurs when Symantec Data Loss Prevention attempts to decode characters from the unsupported character set to a Unicode encoding for analysis. For a list of supported Java 6 encodings please refer to: http://java.sun.com/javase/6/docs/technotes/guides/intl/encoding.doc.html	None.
2752691	Incidents are not created when an email is sent containing an attachment where the file name contains sensitive data that is written using I18N characters.	None.