Symantec™ Data Loss Prevention Release Notes

Version 12.0.1

Symantec Data Loss Prevention Release Notes

Documentation version: 12.0.1a

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- 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 website 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, DVDs, 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

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About these release notes

This document contains important and late-breaking information about Symantec Data Loss Prevention version 12.0.1.

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=56275

What's new in Symantec Data Loss Prevention 12.0.1

In addition to the fixed issues listed in chapter 2, Symantec Data Loss Prevention 12.0.1 includes the following new features:

- Support for Microsoft Windows 8 PC operating systems

- New agent monitoring support for web browsers
- Support for Secure ICAP
- Support for content removal for the Box.com file-sharing service

Each of these features is described here in greater detail.

Support for Microsoft Windows 8 PC operating systems

Symantec Data Loss Prevention version 12.0.1 supports applications running in the Microsoft Windows 8 desktop environment (32-bit or 64-bit) for PCs. Support for desktop apps in Windows 8 is similar to the support for Windows 7, with the following known issues:

- You cannot install the DLP Agent using the default installer. To install the DLP Agent, add the parameter `Allow2003=Yes` to the `InstallAgent.bat` file, then install the agent from the command line.
- Some DLLs may not be removed when you uninstall the DLP Agent. To clean up these files, restart the endpoint computer.

Symantec Data Loss Prevention is not supported for Windows Store (also known as Metro-based) applications. While detection can still occur and incidents are created, there are limitations and known issues related to the detection of Windows Store applications. Symantec Technical Support will not resolve issues that are specific to using Symantec Data Loss Prevention for detecting content and activities of Windows Store applications.

Although Symantec Data Loss Prevention does not support detection for Windows Store apps, incidents are created (if there are policy violations) when such apps are used. The following issues apply to Symantec Data Loss Prevention when Windows Store apps are used:

- Monitoring does not work for FTP, HTTP, HTTPS, print, or Clipboard.
- Application File Access monitoring does not work.
- Policy violations in Windows Store apps create corresponding pop-up windows in the desktop environment.
- Incidents reported from any Windows Store app appear with the application name `RuntimeBroker.exe`.

See “Microsoft Windows 8 desktop known issues” on page 41.

New agent monitoring support for web browsers

Symantec Data Loss Prevention 12.0.1 agents support monitoring of HTTP and HTTPS traffic on Microsoft Internet Explorer versions 8 through 10 and Mozilla

Firefox through version 21. The ability of the DLP Agent to monitor data transfer in a web browser depends on the communication protocol used by a given website. Because many websites use custom application-level communication protocols, Symantec Data Loss Prevention may not monitor traffic to all possible websites.

Support for Secure ICAP

Symantec has certified the Stunnel process to provide a secure communications channel (SICAP) for Data Loss Prevention Network Prevent for Web version 12.0.1. Use of the Stunnel external process allows for a secure communications channel between a Network Prevent for Web Server and a Blue Coat ProxySG. For more information about setting up and configuring the Blue Coat ProxySG and Stunnel to enable secure ICAP functionality with Network Prevent for Web, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* online at the following URL:

https://kb-vontu.altiris.com/article.asp?article=56276

Support for content removal for the Box.com file-sharing service

Symantec Data Loss Prevention 12.0.1 supports content removal for the Box.com file-sharing service.

About accessing Oracle configuration files

The location of files for configuring Oracle for use with Symantec Data Loss Prevention has changed from previous releases. These configuration files, including the database template file and the database user SQL script, are part of your platform ZIP file:`Symantec_DLP_12.0.1_Platform_Win.zip` or `Symantec_DLP_12.0.1_Platform_Lin.zip`.

After you download the platform ZIP file from FileConnect and extract the contents, locate the `Oracle_Configuration` folder. The folder contains the compressed file (`11g_r2_64_bit_Installation_Tools.tar.gz` for Linux platforms, and`11g_r2_64_bit_Installation_Tools.zip` for Windows platforms) that includes the Oracle configuration files.

The *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* included with the downloadable documentation on FileConnect incorrectly identifies the location of the Oracle configuration files. While the correct location is provided in these release notes, you can also download an updated version of the guide at the Symantec Data Loss Prevention Knowledgebase: https://kb-vontu.altiris.com/article.asp?article=56403&p=4.

Installing Symantec Data Loss Prevention

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=56276

When you are ready to install Symantec Data Loss Prevention, refer to the *Symantec Data Loss Prevention Installation Guide*.

Upgrading to the latest release

Upgrading your deployment may involve several different upgrade processes, for the Enforce Server, detection server, the DLP Agent, and Oracle. For detailed information about upgrading to the latest release of Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Upgrade Guide*.

The name of the Upgrader file is incorrect in the Upgrade Guides. To download and extract the Upgrader software, follow these procedures:

To download the upgrade software

1. Download *Acquiring Symantec Data Loss Prevention Software* from Symantec File Connect after registering your serial number certificates at the Licensing Portal. Follow the directions in that document to acquire the Symantec Data Loss Prevention software.
2. Download the ZIP file for your operating system:
   `Symantec_DLP_12.0.1_Platform_Win-IN.zip` or
   `Symantec_DLP_12.0.1_Platform_Lin-IN.zip`.
3. Copy the ZIP file onto the computer from which you intend to perform the upgrade. That computer must have a reliable network connection to the Enforce Server.

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

To extract the ZIP file

1. Extract the contents of the ZIP file you downloaded. Among other items, the ZIP file contains the `Upgrade_12.0_to_12.0.1` folder, which contains an upgrade JAR (Java archive) file that is required later when you run the Upgrade Wizard.
2. Note where you saved the upgrade JAR file so you can quickly find it later.

About Symantec DLP Agent version upgrades

You can upgrade Symantec DLP Agents from one version to another by using an unattended upgrade process, or you can update the agents manually. Manual upgrades are not recommended for large deployments. You can upgrade Symantec DLP Agents as a group if you upgrade using systems management software. If you upgrade the agents manually, you must upgrade each agent individually.

Endpoint Servers are backward-compatible for one full release with an associated Symantec Data Loss Prevention Agent. For example, you may have a version 12.x Endpoint Server and a version 11.x Symantec Data Loss Prevention Agent. These versions are compatible.

Symantec Data Loss Prevention 12.0.1 includes a major agent upgrade. If you are upgrading your Symantec Data Loss Prevention Agents to version 12.0.1 from version 11.6.2 or earlier, you must run the major upgrade MSI package, which will uninstall your old agents before installing the new ones.

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

The following table provides a general overview of the upgrade process:

Table 1-1 Upgrade process for Symantec DLP Agents

Step	Description	Process
1	Download the Symantec Data Loss Prevention Agent upgrade package.	Download the upgrade package from Symantec FileConnect. See the *Symantec Data Loss Prevention Upgrade Guide* for more details.
2	Install the upgrade package on your endpoint computers.	Choose one of the following installation methods: ■ Upgrade the Symantec DLP Agent by using unattended upgrades. ■ Upgrade the Symantec DLP Agent manually.

Table 1-1 Upgrade process for Symantec DLP Agents *(continued)*

Step	Description	Process
3	Optional: restart the DLP Agents to clean up outdated drivers.	You can restart the DLP Agents by using the Enforce Server administration console.

See the *Symantec Data Loss Prevention Upgrade Guide* for more information about upgrading your Symantec DLP Agents to version 12.0.1.

About upgrading the SharePoint Solution

Symantec Data Loss Prevention version 12.0.1 is compatible with the 12.0 version of the SharePoint Solution. The full SharePoint Solution compatibility list is as follows:

Table 1-2 Symantec SharePoint Solution version compatibility

Symantec SharePoint Solution version	Compatible Symantec Data Loss Prevention versions
No version number	11.0 through 11.1.2
11.5	11.5
11.5.1	11.5.1
11.6	11.6, 11.6.1, 11.6.2
12.0	12.0, 12.0.1

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

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

Fixed Issues

This chapter includes the following topics:

Fixed in version 12.0.1

This section lists fixed issues in version 12.0.1. Unless otherwise noted, all issues are fixed on the server side.

Detection issues fixed in 12.0.1

Table 2-1

Issue ID	Description
3237649	The file reader occasionally restarted continuously on the Endpoint Prevent server when IDM policies were enabled.
3237651	When using a policy to detect email attachments, Symantec Data Loss Prevention treated all emails as though they contained an attachment.
3237656	Symantec Data Loss Prevention did not properly normalize fullwidth characters in email subject lines.
3238631	Symantec Data Loss Prevention took a very long time to process detection on surrogate Unicode characters.
3238885	Network Discover failed to generate incidents when using custom data identifiers.
3238887	The file reader failed to start after adding a policy including a response rule with an endpoint device.

Table 2-1 *(continued)*

Issue ID	Description
3238890	Network Monitor failed to detect message attachments with file names containing fullwidth characters.

Discover issues fixed in 12.0.1

Table 2-2

Issue ID	Description
3228345	When you selected the **Scan Status** for a scan that was run a large number of times before your latest upgrade, the Enforce Server administrative interface displayed an error screen and was unable display the **Scan Detail** page.

Endpoint issues fixed in 12.0.1

Table 2-3

Issue ID	Description
3193772	Symantec Data Loss Prevention 12.0.1 includes additional logging information for data identifiers: total number of global data identifiers, total number of patterns in global data identifier list, and number of unique patterns. This is an agent-side fix.
3237653	Data Identifier detection on the endpoint performed poorly compared to detection on the server. This is an agent-side fix.
3237657	Symantec Data Loss Prevention now interprets the content-disposition parameter and submits the corresponding file for detection. This is an agent-side fix.
3238893	Windows Explorer quit unexpectedly on the endpoint computer when uninstalling the endpoint agent while copying files to a network share. This is an agent-side fix.
3238894	Detection failed to detect `.lzh` files on endpoint computers. This is an agent-side fix.
3238895	ZIP files containing sub-file names in UTF-8 were not properly decoded on the endpoint. This is an agent-side fix.

Table 2-3 *(continued)*

Issue ID	Description
3238907	Endpoint Prevent did not detect policy violations on CD/DVD activity if file path filtering was enabled on the CD/DVD monitoring channel. This is an agent-side fix.
3238910	The 32-bit DLP Agent quit unexpectedly when formatting an error string due to invalid arguments.
3238919	The **Ignore File Type** pre-filter did not work as expected with `.doc` and `.txt` file types. This is an agent-side fix.
3238921	On Windows 7 systems, the file system driver `vfsmfd` occasionally caused the endpoint computer to quit unexpectedly when the verifier was enabled. This is an agent-side fix.
3238923	The endpoint agent process quit unexpectedly when performing an Endpoint Discover scan. This is an agent-side fix.
3238932	An incorrect format string caused heap-corruption issues in endpoint detection. This is an agent-side fix.
3238939	Endpoint agent dump file generation has been improved with the addition of exception information. This is an agent-side fix.
3238942	If Microsoft Outlook included a local distribution list that was blank, sending email to any local distribution list caused Outlook to quit unexpectedly. This is an agent-side fix.

Enforce issues fixed in 12.0.1

Table 2-4

Issue ID	Description
3238626	When selecting the **Set Attribute** action after selecting all incidents in an incident list, the Enforce Server administrative interface was unable to render the incident list page.
3238628	The web archive incident list did not include the incident type image.
3238877	Non-administrative users could not export a single summary of Endpoint incidents to a CSV file.
3228889	Symantec Data Loss Prevention returned a syntax error when creating an IP filter on the **Agent Configuration** page with more than four IP addresses.

Table 2-4 *(continued)*

Issue ID	Description
3238913	While processing very large incidents, the Incident Persister failed to process other incidents in the queue.
3238926	Excluding users from role-based access to Application File Access incidents did not work as expected. Such users could only see Endpoint incidents.
3246738	The JCIFS library has been updated to allow you to reset the last-accessed date of a file and retrieve file owner data from computers on the Linux platform.

Installation and upgrade issues fixed in 12.0.1

Table 2-5

Issue ID	Description
3238915	The release update upgrader did not validate the version being upgraded against the supported upgrade versions.

Network issues fixed in 12.0.1

Table 2-6

Issue ID	Description
3238884	Network Prevent for Email removed the SIZE parameter from the ESMTP handshake if the parameter was specified with a numerical value.
3238883	The request processor timeout did not work properly when a `RequestProcessorListener` for the request processor thread was running detection on a previously queued message.
3238911	Network Prevent for Email removed the domain and host information from EHLO responses received from downstream MTAs.
3238917	Network Prevent for Email quit unexpectedly when processing email with multi-line banners.
3238941	Symantec Data Loss Prevention 11.6.3 includes improved ICAP request handling for non-redacted content.

Chapter 3

Known Issues

This chapter includes the following topics:

- Mobile Prevent internationalization and localization known issues

Known product issues

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

Detection known issues

Table 3-1 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.
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.”

Table 3-1 Detection known issues *(continued)*

Issue ID	Description	Workaround
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.
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.
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.
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.

Table 3-1 Detection known issues *(continued)*

Issue ID	Description	Workaround
2174291	Symantec Data Loss Prevention does not clean up EDM indexes that are split across multiple files.	In the `Indexer.properties` file, increase the value of `max_loaded_index_memory` to accommodate the entire EDM index in a single file.
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.
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.
2620725	EDM strips alphabetic characters from the end of five-digit strings, resulting in false-positive matches.	None.
2711768	If you configure a keyword condition in a policy to match on email subject lines, the detection engine may fail to generate incidents if the message contains a MIME encoded-word subject line.	None.
2923517	Symantec Data Loss Prevention does not detect keywords in files authored in Hangul 2010 SE+.	None.
2988383	The VML training phase occasionally hangs at step one after having trained other VML profiles.	None.

Table 3-1 Detection known issues *(continued)*

Issue ID	Description	Workaround
2989573	For keyword policies, Symantec Data Loss Prevention returns incident match counts that are one greater than the maximum match count value. For example, if you have set the maximum match count to 100, Symantec Data Loss Prevention returns an incident match count of 101.	None.

Discover known issues

Table 3-2 Discover known issues

Issue ID	Description	Workaround
2529816, 2531206	Some items on broadcast sites created with Microsoft Web Apps on SharePoint 2010 and 2013 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.
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.

Table 3-2 Discover known issues *(continued)*

Issue ID	Description	Workaround
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 12.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.
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.

Table 3-2 Discover known issues *(continued)*

Issue ID	Description	Workaround
2483068	The "Ignore smaller than" filter may not work for certain smaller files on Microsoft Exchange 2010 targets. Because Exchange email files are scanned by Network Discover in both plain text and HTML format, the file size represented in the target list page is larger than the actual file in Exchange.	None.
2497863	The Open In Browser link does not work for archived mailbox items.	None.
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.
2941562	If you stop a Content Root Enumeration scan, the elapsed time displays as zero.	Allow the scan to run to completion, and the elapsed time will display correctly.
2943550	Network Discover does not scan files without an extension on Unix/Linux systems.	In the `VontuFileSystemScanner.cfg` file on your Discover server, add a wildcard value to the `DirectoryFileMatch` parameter: `DirectoryFileMatch=*`
2980582	The column named "Protect Status" on the incident view page is named "Message Status" when you export the incident to a CSV file.	None.
2988284	Symantec Data Loss Prevention does not reset the last-accessed date for files on Linux systems.	None.

Table 3-2 Discover known issues *(continued)*

Issue ID	Description	Workaround
3035527	The scanner installation file overwrites existing scanner installations without displaying a warning message.	None.
3050222	The File System Scanner will not run as a service on AIX systems.	Install the File System Scanner as an application, not a service.
3082527	If the Discover Server runs out of disk space while running an incremental scan, the incremental scan becomes stuck in the Running state.	Clear some disk space on your Discover Server, then the scan will automatically resume.
3182043	When you click the **Go to Data Insight** link on a Symantec Data Loss Prevention incident, the workspace path on the Symantec Data Insight console is not expanded to the file level.	None.
3182510	If Symantec Endpoint Prevention is installed on your Discover Server, your Discover remote target scans will not work	Whitelist the ports connecting your Discover Server to your Discover remote scanner targets in the Symantec Endpoint Protection firewall settings.
3206907	When scanning ASPX pages on SharePoint 2013 sites, some HTML text (for example, "_objectType_") may appear in your incident snapshots.	None.

Documentation known issues

Table 3-3

Issue ID	Description	Workaround
2729277	The documentation for metadata detection in chapter 33 (“Detecting Document Metadata") of the *Symantec Data Loss Prevention Administration Guide* indicates that metadata extraction is the same for files on servers and endpoints. However, this may not always be the case. For example, a custom metadata tag in an XLS file is truncated to one character when extracted on the endpoint, whereas on the server the full metadata tag is extracted.	None.

Table 3-3 *(continued)*

Issue ID	Description	Workaround
N/A	The name of the Upgrader file is incorrect in the *Symantec Data Loss Prevention Upgrade Guide*.	The Upgrader JAR file is available in the `Upgrade_11.x_to_12.0` directory in the Platform ZIP file for your operating system: `Symantec_DLP_12.0_Platform_Win-IN.zip` or `Symantec_DLP_12.0_Platform_Lin-IN.zip`.
3081126	On page 1134 of the *Symantec Data Loss Prevention Administration Guide* in the section on enabling GET processing with Network Prevent for Web, references to the Network Monitor Server are incorrect. The referenced server should be Network Prevent for Web	None.
3220350	The *Symantec Data Loss Prevention Administration Guide* incorrectly states the Endpoint Prevent support for monitoring virtual desktops, on page 1310 in the topic "About virtual desktop support with Endpoint Prevent." Endpoint Prevent in version 12.0 does not support Microsoft Hyper-V virtualization server, Microsoft Remote Desktop Services, or VMware View virtualization server.	None.
3229499	The *Symantec Data Loss Prevention Administration Guide*, in the topic "About Endpoint Discover monitoring," incorrectly states that you cannot automatically remediate Endpoint Discover incidents. You can use the automatic quarantine response rule for Endpoint Discover incidents or create a custom response using the Endpoint FlexResponse API. See the *Symantec Data Loss Prevention Endpoint FlexResponse Plug-in Developers Guide* for details.	None.
3241424	The *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* incorrectly states that `Oracle_11.2.0.3.0_Server_Installation_Tools_Lin.zip` is a file that needs to be downloaded from FileConnect for Linux deployments.	The configuration files for using Oracle with Symantec Data Loss Prevention are now included in your platform ZIP file, `Symantec_DLP_12.0_Platform_OS.zip`. After you extract the platform ZIP file, the `Oracle_Configuration` folder contains the compressed file with the configuration files within: ■ `11g_r2_64_bit_Installation_Tools.tar.gz` for Linux platforms ■ `11g_r2_64_bit_Installation_Tools.zip` for Windows platforms

Table 3-3 *(continued)*

Issue ID	Description	Workaround
3242444	On page 22 of the *Symantec Data Loss Prevention Upgrade Guide for Windows*, the path to the `Manager.properties` file is incorrect.	The correct path to the `Manager.properties` file is `\SymantecDLP\Protect\config\Manager.properties`.
3255207	On page 959 of the *Symantec Data Loss Prevention Administration Guide*, the following note appears: "Note: The XML schema files for exported reports are located in the `c:\Vontu\Protect\tomcat\webapps\ProtectManager\WEB-INF\lib\reportingapi-schema.jar` file." The file path specified in this note is incorrect.	The correct path is provided in the *Symantec Data Loss Prevention Incident Update and Reporting API Developers Guide*: `C:\SymantecDLP\Protect\tomcat\lib\incidentapi-2011-schema.jar`

Endpoint known issues

Table 3-4 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.
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 ■ l0020126407 ■ 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.

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

Issue ID	Description	Workaround
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.
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.	None.

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

Issue ID	Description	Workaround
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.	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.
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 it contains sensitive information.	None.
2100592	If the Symantec DLP Agent is stopped during a USB data transfer, Windows Explorer crashes.	None.
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.

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

Issue ID	Description	Workaround
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.
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.

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

Issue ID	Description	Workaround
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.
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.
2545486, 2529385	Toshiba eSATA devices are detected as local drives rather than as removable drives.	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.

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

Issue ID	Description	Workaround
2656696	Symantec Data Loss Prevention does not detect policy violations for documents saved to the root directory of a publised drive in Citrix XenApp 6.5.	None.
2724448	Symantec Data Loss Prevention does not detect bitmaps when they are sent as inline images through Lotus Notes.	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.
2858675	File type filters do not ignore the `.ipa` file type if they are specified in the **Ignore Filter** list.	None.
2980734	Symantec Data Loss Prevention does not detect or block files that an endpoint user uploads using Internet Explorer to http://files.mail.ru.	Enable Application File Access monitoring for file reads on Internet Explorer.
3182794	The default value for three Endpoint configuration settings have changed in Symantec Data Loss Prevention version 12.0. If you are upgrading from a previous version with values for these settings below the new default values, your existing values will be overwritten. The settings and new default values are: ■ Endpoint Discover target **Scan idle timeout** setting: one hour ■ Endpoint Agent advanced setting `Discover.STANDARD_REPORT_INTERVAL.int`: 60000 milliseconds ■ Endpoint Server advanced setting `EndpointServer.Discover.ScanStatusBatchInterval`: 60000 milliseconds	None.
3182827	If any DLP Endpoint Discover scans are running during an Enforce Server upgrade, they will continue to run after the upgrade is complete regardless of the status of the Endpoint agent. The scan will never complete, though it will eventually time out as an idle scan.	Stop any running DLP Endpoint Discover scans before upgrading your Enforce Server.

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

Issue ID	Description	Workaround
3297031	HTTP and HTTPS monitoring of some websites may generate incidents continuously when the `Block` or `User Cancel` response rules are triggered. This behavior is common for Gmail and Yahoo.	None.
3297049	The **Notify** pop-up window occasionally does not appear when email containing a sensitive keyword is sent over HTTPS from Gmail or Yahoo using Microsoft Internet Explorer.	None.

Enforce Server known issues

Table 3-5 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.

Table 3-5 Enforce Server known issues *(continued)*

Issue ID	Description	Workaround
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.
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.
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.

Table 3-5 Enforce Server known issues *(continued)*

Issue ID	Description	Workaround
2610462	On the **Create User Groups** page, the scroll bar 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.
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.
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.
2920529	Using the **Select All** button with the **Set Attribute**action from the incident list page causes Symantec Data Loss Prevention to quit unexpectedly.	To set attributes for multiple incidents from the incident list page, click **Show All**, then select the incidents using the checkboxes.
3159391	The default reports for roles defined in solution packs are incorrect.	None.
3200251	If you have configured the Enforce Server to **Send reports as links, login required to view** and then use **Send Now** to send a saved report, the report recipient receives this error message when they click the report URL: "The report you are trying to access has been deleted."	Do not use **Send Now**. Instead, use **Schedule Distribution**, set the frequency to **Once**, and set the send time for some time in the past. This method will distribute the correct report URL immediately.

Installer and Upgrader known issues

Table 3-6 Installer and Upgrader known issues

Issue ID	Description	Workaround
1719273	When upgrading DLP Endpoint agents, 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.	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 3-6 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 `\SymantecDLP\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.

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**.
2894970	If you are installing Symantec Data Loss Prevention from the command line on Linux systems and the connection to Oracle fails, you cannot exit the installation process.	To work around this issue, follow this procedure: 1 Run `ps -Hu protect` to get the PID for the `upgrader-java` process. 2 Run `kill -9 PID` 3 Delete all files from the /SymantecDLP/ directory. 4 Remove all SymantecDLP services: `rm -f /etc/init.d/SymantecDLP`. 5 Remove the Protect user: `userdel -r protect`.

Table 3-6 Installer and Upgrader known issues *(continued)*

Issue ID	Description	Workaround
3096239	If the database connection fails during the installation process, the installer exits without cleaning up its files. Any subsequent installation will fail with a duplicate license error.	To work around this problem, clean up the remaining files using this procedure: 1 Delete all files from the /SymantecDLP/ directory. 2 Remove all SymantecDLP services: ■ On Linux: `rm -f /etc/init.d/SymantecDLP` ■ On Windows: `sc delete Service Name` 3 Remove all users: ■ On Linux: `userdel -r protect` ■ On Windows: remove the `protect` and `protect_updates` users from the Local Users and Groups tab in the Computer Management administrative tool
3120181	Installation fails if the Symantec Data Loss Prevention Administrator password contains an ampersand (&) character.	None. Delete the `/SymantecDLP/` directory and any of its contents, then run the installer again using an Administrator password without an ampersand (&) character.
3136083, 3160608	Upgrades will fail if any Enforce or Detection Server files are being edited by a separate process, or if those files do not have the proper permissions.	Ensure that you have the correct permissions set for all Enforce and Detection Server files, and that no files are open for edits before starting the upgrade process.

Lookup plug-in known issues

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

Table 3-7 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**.

Microsoft Windows 8 desktop known issues

Table 3-8

Issue ID	Description	Workaround
3297986	In Windows 8, some DLLs may not be removed when you uninstall the DLP Agent.	To clean up these files, restart the endpoint computer.
3298461	In Windows 8, you cannot install the DLP Agent using the default installer.	Add this parameter to the agent installation batch file script (`InstallAgent.bat`): `Allow2003=Yes` Then install the agent from the command line.

Mobile Prevent known issues

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

Table 3-9 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.

Table 3-9 Mobile Prevent known issues *(continued)*

Issue ID	Description	Workaround
2628239	The iCloud iPad application is not supported.	None.
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**.
2746202	Mobile Prevent does not detect non-ASCII character keywords when sending email using a Gmail ActiveSync account on an iOS device.	None.
2975095	Symantec Data Loss Prevention does not detect policy violations in attachments when searching email on the server side from iOS devices.	None.

Network known issues

Table 3-10 Network known issues

Issue ID	Description	Workaround
N/A	For Network Incident Reports: When adding a filter in Advanced Filters and Summarization, and choosing Environment in the first field, the “Show Cloud Incidents” and “Show On Premises Incidents” options appear in the second field; these options are not available for use in version 12.0.	None.
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.
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 3-10 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.
2910319	You cannot sort Network or Mobile incidents by recipient.	None.
2980596	When monitoring SMTP with command pipelining enabled, Network Monitor may treat the RSET command as part of the message body.	Disable SMTP command pipelining on your MTAs.

Table 3-10 Network known issues *(continued)*

Issue ID	Description	Workaround
3181662	On Windows 2008R2 systems using standard network interface cards such as Broadcom or Intel Server Cards, the Symantec Endpoint Protection (SEP) version 12 firewall may interfere with Network Monitor operation . The SEP firewall does not affect Network Monitor when using the Napatech NT4E card.	Take one of the following actions: ■ Opt out of the firewall component during the SEP installation process. ■ Disable the firewall on an existing SEP installation. ■ Configure the SEP firewall to allow IP traffic in **Unmatched IP Traffic Settings**.

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 3-11 Detection internationalization and localization known issues

Issue ID	Description	Workaround
1404046	Archive files such as zip that contain files that violate a policy will appear in the incident snapshot. The files within the archive may appear with garbled names if the names use non-ASCII characters.	None.
1476390	Symantec Data Loss Prevention does not detect match DBCS characters in Unicode HTML files copied to USB drives.	None.
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.

Table 3-11 Detection internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
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.
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.

Table 3-11 Detection internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
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.
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.
1894279	Symantec Data Loss Prevention does not detect attached files with DBCS file names.	None.
2075491	Detection of files copied to USB or local drives fails when Endpoint agents are installed in HI-ASCII folders.	
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.

Table 3-11 Detection internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
2371246	Symantec Data Loss Prevention Endpoint agents treat Korean as a non-whitespace language. This issue causes Endpoint detection on Korean-language content to be less accurate.	None.
3114433	Symantec Data Loss Prevention does not detect Shift_JIS encoded text (`.txt`)files.	None.

Discover internationalization and localization known issues

Table 3-12 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.
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.

Table 3-12 Discover internationalization and localization known issues *(continued)*

Issue ID	Description	Workaround
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 3-13 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 the way 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 3-14 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 3-15 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 3-16 Network internationalization and localization known issues

Issue ID	Description	Workaround
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.

Mobile Prevent internationalization and localization known issues

Table 3-17 Mobile internationalization and localization known issues

Issue ID	Description	Workaround
2582425	Non-ASCII data in the body and subject of an email may not get inspected when sent to Gmail through the iPad Safari web browser. Mobile Prevent cannot detect the encoding mechanism that is used by Safari.	None.
2597883	When transmitting data from an iPad, Mobile Prevent fails to detect data stored in text files encoded with `x-mac-cyrillic`.	None.
2920361	Mobile Prevent does not display a localized version of attachment names.	None.
3040853	Mail sent from Exchange Server 2010 mail accounts that contain French keyword violations appear corrupted on the incident page.	None.