Release Notes

Symantec Data Loss Prevention 11.0

Last updated: December 3, 2010

These Release Notes cover the following topics:

- Introduction
- What's new
- Product documentation
- Known issues
- Internationalization and localization known issues

Introduction

This document contains information regarding known issues for the v11.0 release of Symantec Data Loss Prevention.

Before installing Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide*. This guide contains information on the requirements needed to deploy Symantec Data Loss Prevention.

When you are ready to install Symantec Data Loss Prevention, use the *Symantec Data Loss Prevention Installation Guide*. You can install on Windows or Linux operating systems.

There are new product guides for v11.0. Please see the list in the "Product documentation" section, later in these release notes, for all of the available product guides in v11.0.

You can view the most current version of the Release Notes on the Altiris Knowledgebase. Log on and search for article 54147.

What's new

The following features are new for the v11.0 release ofSymantec Data Loss Prevention:

- 64-bit operating system support
- Oracle 11g support
- Network Prevent installation to a hosted environment
- Flexible upgrade window for detection servers
- Endpoint Discover Quarantine response rule
- Application monitoring
- Improved agent troubleshooting tasks
- Endpoint Prevention for Network Shares
- Content aware device control
- Endpoint FlexResponse
- Rules results caching
- Improved agent health statuses
- Folder risk reporting
- Data-owner remediation reports
- Enhanced SharePoint scanning
- High-speed packet capture for Network Monitor
- New Classification detection server
- Incremental scanning
- Enhanced Exchange scanning
- Extensible Data Identifiers
- Hosted deployment for Network Prevent
- High-speed packet capture for Network Monitor
- Network Prevent (Web) support for Symantec Web Gateway
- Server-side group-based policies
- Keyword proximity matching and wildcard character
- Data owner exception
- Content Extraction API
- Authorized endpoint devices
- Detection for data classification services
- Response rule ordering
- Subject message component

New features for the v11.0 release are discussed in detail in Chapter 1 of the *Symantec Data Loss Prevention Upgrade Guide*.

Product documentation

The documentation for v11.0 includes the following:

- *Symantec Data Loss Prevention System Requirements and Compatibility Guide*
- *Symantec Data Loss Prevention Administration Guide*
- *Symantec Data Loss Prevention Installation Guide for Windows*
- *Symantec Data Loss Prevention Installation Guide for Linux*
- *Symantec Data Loss Prevention Upgrade Guide for Windows*
- *Symantec Data Loss Prevention Upgrade Guide for Linux*
- *Symantec Data Loss Prevention Reporting API Developers Guide*
- *Symantec Data Loss Prevention Server FlexResponse Platform Developers Guide*
- *Symantec Data Loss Prevention Integration Guide for Microsoft Internet Security and Acceleration Server*
- *Symantec Data Loss Prevention MTA Integration Guide for Network Prevent (Email)*
- *Symantec Data Loss Prevention Integration Guide for Squid Web Proxy*
- *Symantec Data Loss Prevention Lookup Plug-in Guide*
- *Symantec Data Loss Prevention Network Monitor and Prevent Performance Sizing Guidelines*
- *Symantec Data Loss Prevention System Maintenance Guide*
- *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide*
- *Symantec Data Loss Prevention Detection Customization Guide*
- *Symantec Data Loss Prevention Data Insight Implementation Guide*
- *Symantec Data Loss Prevention Solution Packs*
- *Symantec Data Loss Prevention Third-Party License Agreements*
- Symantec Data Loss Prevention online Help

After you've downloaded and unzipped the Symantec_DLP_11.0_Docs_<OS_platform>-IN.zip file, you can find PDF product documentation in

`DownloadHome/DLP/Symantec_DLP_10_<OS>/11.0_<OS>/Docs/,`

where *DownloadHome* is the specific download path you’ve chosen, *<OS>* is your specific operating system (either Linux or Windows).

In addition, you can find information about the product in the online Help.

Known issues

The following issues are known issues in 11.0. Where possible, a workaround is provided. The boldface number associated with each issue is an internal reference number.

Classification

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 reboots, the incident total for the server can increase up to the sum of the threshold amounts, even though no new incidents are actually added to the Enforce Server database.

Workaround: None.

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.

Workaround: In the detection rule definition for Classification Policies, deselect the Envelope option and select the Subject option.

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.

Workaround: None.

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.

Workaround: None.

2185534

When configuring a Detection condition on a Data Classification Server to match on only the body of a message, mail items that only match attachments may be classified. If the condition is configured only for attachments, the body of attached messages is not part of the detection.

Workaround: None.

Detection

1826457

DGM policies based on EDM profiles do not detect email messages formatted by Lotus Notes.

Workaround: None.

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**).

Workaround: A plug-in using the Content Extraction API can be used.

2129686

You cannot import v10.x policies containing Data Identifier or Keyword Matching rules or exceptions to the v11 Enforce Server.

Workaround: See the topic "Importing v10 DI and Keyword policies to v11 systems" in the v11.0 documentation.

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.

Workaround: Use a Data Identifier condition with a Custom File Type Signature condition to detect precise data from custom file types on the endpoint.

2177541

The ContentExtraction.MaxContentSize Advanced Server Setting does not apply to the text file type (*.txt).

Workaround: None.

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.

Workaround: None.

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.

Workaround: None.

Discover

1520235

While running Scanner target scans (SharePoint, Exchange, File System, LiveLink, Documentum, or Web Server) in parallel, when one of the scans finishes the remaining running scans might stop processing data. When this happens, statistics for the scan stop updating (the Items Scanned and Bytes Scanned data) on the Discover Targets screen. If you suspect a scan has stalled on the Scanner machine, check to see if there are any new HTTP posts. You can also check to see if there is a Tomcat exception in the file reader logs.

Workaround: On the Discover Targets screen, pause the scan, then resume the scan.

1961596

Network Protect (copy or quarantine) does not work on Windows 2008 DFS file shares. Network Protect works on Windows 2003 DFS file shares.

Workaround: 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.

Workaround: None.

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.

Workaround: 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:

! # $ ' - ^ _ ' { }

Workaround: 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 popup blocker in Microsoft Internet Explorer 8.

Workaround: When the Internet Explorer 8 popup blocker displays a warning near the top of the browser window, click on the warning and choose to always allow popups 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.

Workaround: 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.

Workaround: 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.

Workaround: 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.

Workaround: Create a separate target for the content root with the blank credentials. Set the default user credentials to blank for that target.

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 used.

Workaround: 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.

Workaround: None.

Endpoint

1510556

Sensitive information can be printed as a .pdf file if it is sent through the Adobe PDF Converter. For example, if you have a Microsoft Word document containing sensitive information and you create a PDF by selecting the Print to PDF option, then a .pdf file of the page containing the sensitive information is created. Although a block notification is shown and a corresponding incident is created, the page on which the sensitive text is found is printed into a PDF. However, none of the pages after that first sensitive page are printed.

Workaround: None.

1523460

Uninstalling any version of the Symantec DLP Agent and then installing the Symantec DLP Agent again, without rebooting the endpoint machine after the uninstall and before the re-install, causes the agent install to fail silently.

Workaround: You must reboot the endpoint machine after uninstalling the Symantec DLP Agent before you can install the Symantec DLP Agent again.

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.

Workaround: You must manually delete any files that have not been deleted.

1719273

SEP Tamper protection messages are displayed on upgrading Endpoint Agent from v10.x to v11.0

These messages appear every time the agent service is restarted.

Workaround: Re-install Symantec DLP Agent V11.0.

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.

Workaround: Close 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

I0020126407

i0020126407

c0000763012

Although the data contains different cases, it is essentially the same. Endpoint agents regard each case as a separate instance.

Workaround: Create an endpoint regular expression policy that contains both case sensitive and case insensitive versions of the regular expression.

1799071

If multiple recipients are specified in the **Recipient Pattern** field and the MatchCounting option is greater than 1, then 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.

Workaround: When creating the Recipient Pattern rule, set MatchCounting to “At least 1 recipient must match.”

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.

Workaround: None.

1851220

Endpoint Email/SMTP cross-component matching of compound EDM or IDM policies does not work when the keyword or regex 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.

Workaround: 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.

Workaround: After compounding the DCM exception to a Context type exception, change the default selection from “Matched Components” to “Entire Message”.

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.

Workaround: None.

1902505

If the file extension filter configuration is not correct, if it contains commas or other non-newline separators, no error message is displayed to indicate this. If the configuration is not correct, the file extension filters will not work.

Workaround: Ensure that file extension filters are separated **only** with newlines, and not with any other characters such as commas, semicolons, or any other punctuation.

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.

Workaround: Use third-party CD/DVD burning software.

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.

Workaround: None.

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.

Workaround: None.

1975097, 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.

Workaround:

Use one of the following workarounds:

- Set the **Specify Default Filter Action** setting to **Monitor**.
- Make sure that *.zip files are configured as one of the monitored file types for all monitored devices.

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)

Workaround: None.

1986278, 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 virus and will delete it.

Workaround: White-list clean_agent.exe in Norton Internet security application.

1989339, 1829171

In rare circumstances, incidents on agent can get queued up and will not be pushed to server in a timely manner. For example, this can happen if the file scan experiences unusually high activity.

Workaround: Restart the Symantec DLP Agent.

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 it will not 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.

2078404

Application Monitoring may not be able to block violating files with Read monitoring if a user double clicks to open the file.

Workaround: Use file monitoring in Open mode.

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.

Workaround: For custom DI changes, you can force a change by disabling or enabling the policy on which they depend.

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.

Workaround: None.

2100592

If the Symantec DLP Agent is stopped during a USB data transfer, Windows Explorer crashes.

Workaround: 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.

Workaround: 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.

Workaround: 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.

Workaround: None.

2119984

Citrix publish 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.

Workaround: 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.

Workaround: 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.

Workaround: None.

2129471

The Symantec DLP Agent is not compatible with Symantec Norton products.

Workaround: None.

2131164

There is a possibility that some application will retry to attach file blocked via application monitoring. In such circumstances, endpoint computer users will see multiple pop-ups and multiple incidents will be reported.

Workaround: 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.

Workaround: 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.

Workaround: 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.

Workaround: None.

2146393

The File Size Ignore filter is not supported for any USB removable drives on Citrix XenApp clients.

Workaround: 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

Workaround: 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

Endpoint computers that are marked with an Agent Deployment Status as “Not Managed” are not displayed on the DLP IC Home Page under DLP Agent Deployment status. Nor are they displayed on DLP IC Reports and Filters (Not Managed Computers.)

Workaround: View or use the “Not Managed” endpoint computers through the SMP Filter. The SMP Filter is available under the **Reports >All Reports** tab and by navigating to **Notification Server Management > Agent > All Windows 2000/XP/2003/Vista/2008/7 Computers with No Agent**.

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.

Workaround: After making changes in detection advance settings, disable your policies, wait 30 seconds and re-enable the policy. This causes all the policies to be re-sent and the rule results cache on the endpoint computer is flushed.

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.

Workaround: None.

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.

Workaround: Do not provide alternate Endpoint Servers when you first run the Change Endpoint Server task if the agent is already connected to an alternate Endpoint Server. If alternate servers are needed, add them in a second run of the Change Endpoint Server task. However, on this second run, do not change the primary Endpoint Server.

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.

Workaround: None.

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.

Workaround: Do not use match thresholds with Keyword Proximity conditions.

Endpoint Memory Advisory Note

The Symantec DLP Agent uses memory in a way that maximizes performance. The amount of memory that the Symantec DLP Agent uses varies over time. The Symantec DLP Agent allocates memory in chunks that vary in size depending on the tasks performed. Such tasks include loading policies or detection on large files. After the Symantec DLP Agent finishes a task, memory is gradually released over a period of time. If you observe the amount of memory the Symantec DLP Agent uses, you will typically see memory consumption increase or decrease over time.

Enforce

1529089 version 9.0

For various types of incidents, the Incident Snapshot report shows either the Source IP or the Machine IP. Both of these labels refer to the same thing; the IP address of the host (whether endpoint or other network-based resource) where the incident message originated.

Workaround: None.

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.

Workaround: An Enforce user with System Administrator privileges or the Administrator user should login to the administration console and update the product license field with a valid, current license.

1745611

When making sequential Reporting API Incident List queries with an `oldestIncidentCreationDate` constraint applied, there are cases where it is possible to miss incidents if strict date/time boundaries are used between queries.

Workaround: Use one of the following:

- Apply date filters to the saved report being used for the Incident List query to control which incidents are returned rather than using the `oldestIncidentCreationDate` constraint. For example, by applying a date filter of Yesterday to a saved report and retrieving all incidents for that report on a daily basis through the Incident List query (by not applying an `oldestIncidentCreationDate` constraint), one could ensure that no incidents are missed.
- Use an overlapping time window when making sequential Reporting API Incident List queries. Rather than passing in the date of the last incident retrieved from a prior call, one could instead pass in an `oldestIncidentCreationDate` that represents some amount of overlap with the previous Incident List query. This reduces the chance of missing any incidents but requires that the client consuming the Incident List response filter out duplicate incidents.

1831047

The Original Message component that is retrievable through the Reporting API Incident Binaries query may contain duplicate data.

Workaround: Ignore the duplicate data in the Original Message content. Or, alternately, retrieve the original message through the incident snapshot instead of the Reporting API

2047291

The sslkeytool utility does not run correctly on FIPS-enabled Enforce Servers.

Workaround: None.

2084579

When the Vontu Manager service is shut down, it will log a message similar to the following one:

<date><time>- Servlet MessageBrokerServlet threw unload() exception

javax.servlet.ServletException: Servlet.destroy() for servlet

MessageBrokerServlet threw exception

Workaround: Ignore this message.

2092995

On Linux systems, restarting file access query databases do not sync to the Enforce Server local time zone. Most commonly, the file access query databases are offset to -25200.

Workaround:

Set the default time zone of the Linux JREs by using the TZ environment variable.

1. Add the following to `VontuIncidentPersister.conf:set.TZ=GMT`
2. Restart the Incident Persister service.
3. Replace GMT with the identifier for the desired time zone.
   The timezoneidentifier 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 Vontu 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.

Workaround: 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.

Workaround: Use one of the following workarounds:

- Don't use FIPS mode.
- Disable Liquid Machines Enterprise Rights Management FlexResponse encrypted communications when in FIPS mode.

2148495

Monitor Controller service does not restart automatically after a system restart.

Workaround: Restart Monitor Controller service manually.

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.

Workaround: Use Mozilla Firefox or Microsoft Internet Explorer 8.

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.

Workaround: Rename your detection servers so that they do not contain the “:” symbol.

2165549

Custom Data Identifiers created before version 11.0 are not valid after you upgrade to version 11.0. Incidents that were generated from those identifiers will remain, but the Custom Data Identifier name no longer appears in the incident snapshot.

Workaround: None.

2168915

Editing the same user group from multiple Enforce Server sessions at the same time results in a system-wide failure.

Workaround: None.

Installer

1834598 version 9.0

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.

Workaround:

- Click **Next** and dismiss the error popup 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.

1916802

If an additional, non-English locale is set during the installation of the v10 Enforce Server, the upgrader fails because of non-writable files in the online help directory.

Workaround: If an additional locale was set upon installation, log into Enforce as the root user and execute the following command:

```
chown protect:protect -R /<DLP Installation Directory>/Protect/tomcat/webapps/
ProtectManager/help
```

The default value for <DLP Installation Directory> is */opt/Vontu*.

1975952

Single-tier systems upgraded from 9.x to 10.0 will be missing the inline SMTP keystore configuration property in the Protect.properties file. This causes errors in MTA integration.

Workaround: Add the following lines to the Protect/config/Protect.properties file:

```
Protect.properties does not have the following property in upgraded system,

#SMTP Prevent keystore

com.vontu.inline_smtp.keystore = <install directory>/Protect/keystore/
prevent.ks
```

where *<install directory>* is the path under which your single-tier DLP server is installed.

2148552

There is an error in the RSA BSAFE Crypto-J 4.0 provider that prevents the CA signed certificate chain from being imported.

Workaround: 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.

Prevent

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.

Workaround: None.

1709758

During the uninstallation of the Symantec ISA web-filter plugin, 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.
```

Workaround: There are no known side effects at this time. The symc_isa_plugin.dll is removed properly during uninstall. These errors can be ignored.

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.

Workaround: None.

1887579

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.

Workaround: 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, this 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 highly 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.

Workaround: None.

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.

Workaround: None.

2166589

On 64-bit Windows platforms, Network Monitor cannot monitor VLAN traffic for certain network interfaces.

Workaround: 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.

2176423

Network Monitor does not support 64-bit Endace drivers on Windows platforms.

Workaround: Use native, high-speed packet capture on Windows 64-bit platforms.

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).

Workaround: None.

Upgrader

1719273

When upgrading, Symantec Endpoint Protection (SEP) shows tamper protection alerts when edpa.exe restarts in the presence of the Symantec Management Agent.

Workaround: Add edpa.exe and cui.exe to the SEP tamper protection exception list.

Use the following steps:

1. Login 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.

This workaround is only applicable for managed SEP clients only. Currently, there is no solution for unmanaged SEP clients.

2119435

Group Directories prior to 11.0 do not have indexes associated with them for use in server-side group-based policies.

Workaround: Use the following procedure:

1. After upgrading to 11.0, go to each existing Group Directory connection: **System > Settings > Group Directories > [name of item].**
2. On the **Index Settings** tab, set the desired indexing schedule.
3. Save.

After this is complete and the scheduled indexing jobs have run, the group-based policies using User Groups from those Group Directories will be applied on Detection Servers.

Internationalization and localization known issues

Arabic/Hebrew

1791134, 1866769

Detection for PDF files containing Arabic or Hebrew text fails to detect violations.

Workaround: None.

1791138

Print monitor fails to detect sensitive Arabic data on the Endpoint when printing from applications such as Notepad, Word, and PDF files.

Workaround: None.

1866765

Print monitor fails to detect sensitive Hebrew data on the Endpoint when printing from Notepad.

Workaround: 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.

Workaround: None.

Detection

1308987

When sending an email with HTML content in the body, a Symantec Data Loss Prevention partner handles the text extraction. However, the encoding of the file is not passed through, so the text extraction engine does not convert it correctly to UTF-8.

Workaround: None.

1430029, 1479328

In some cases, when viewing the incident snapshot for an attachment with a non-ASCII filename, the filename may be garbled in the UI.

Workaround: None.

1466323, 1470209, 1470164, 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

Workaround: 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 filenames may be garbled.

Workaround: 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.

Workaround: 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.

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.

Workaround: None.

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.

Workaround: 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.

Workaround: 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).

Workaround: 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 our detection engine.

- Uppercase equivalent of “i” is “I” and not “I”.
- Lowercase equivalent of “I” is “i” and not “i”.

Workaround: Create separate case sensitive policies.s

1833344, 1823548

Regex for Unicode codepoint fails on the endpoint. For example, searching for Unicode character `\u6211` fails. Also the java regex 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.

Workaround: Use the international character in the regex instead of the code point or \w and or `\p{L}` class respectively.

Discover

1704203

Scanner installation on non-English environments has issues when the folder being used for installation (from/ to) has multi-byte characters.

Workaround: Use a folder with non multi-byte ASCII characters when installing the 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.

Workaround: 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.

Workaround: Use a system mounter instead of JCIFS.

1824358

Scanner configuration files do not support Byte Order Mark (BOM) when saved using UTF8 encoding.

Workaround: Use a third party tool such as Notepad++ to save the file without BOM.

1923399

For SharePoint 2007 scanners, `VontuSharePoint2007Scanner.cfg` using non-ASCII values for the MustHaveCSVs parameter does not work.

Workaround: The MustHaveCSVs parameter value must use Percent-Encoding, otherwise known as URI-encoding, if you input non-ASCII values.

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.

Endpoint

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.

Workaround: 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

2152196

The following error message appears if you save reports with non-ASCII characters in the report names:

“Report name is not unique”

Workaround: Use ASCII characters in report names.

2167210

Detection monitors fail to start if the target device name contains non-ASCII characters.

Workaround: Use the following procedure:

1. Open your registry editor:
   `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

1805050

Services fail to start when run by system users with their locale set to Turkish.

Workaround: 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.

Monitor

1466355, 1470241, 1826117

Symantec Data Loss Prevention does not match against DBCS keywords in POP3 or Telnet traffic. POP3 and other custom TCP protocols are designed to extract ASCII text from network traffic. By design, they do not support multi-byte characters. There is a new feature in consideration for future releases to support multi-byte characters.

Workaround: None.

1717416

Non-ASCII content used in Yahoo Messenger over HTTP Proxy may pass through Symantec Data Loss Prevention inspection in Network Prevent for Web deployment.

Workaround: None.

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

Workaround: None.