Release Notes
RSA DLP 9.6

March 26, 2013

Introduction

This document lists the changes that occurred in RSA Data Loss Prevention (DLP) for the 9.6 release. It includes additional installation information, as well as workarounds for known issues. Read this document before installing the software.

What's New

RSA DLP Release 9.6 includes the following new features and functionality:

DLP Endpoint Improvements

- Support for monitoring of iOS devices via iTunes Library.
- Support for monitoring of mobile devices connected using MTP.
- Support for monitoring of internal SD-card and eSATA devices.

DLP Enterprise Manager Improvements

- Support for mapped LDAP user to login to Enterprise Manager console using samAccountName.
- Support for logged in LDAP user to perform manual remediation actions.
- Improvements to Datacenter Grid scan complete status. Users can now map exception to scan status.
- Support for purging matched content only.
- Allow user to view the scan configuration used for a completed scan from the history tab. This information is available only for scans run after upgrading to DLP 9.6.

DLP Datacenter Improvements

- SharePoint Online scans. The DLP Datacenter infrastructure now supports SharePoint Online scans and scan throttling based on the health score of the SharePoint server.

DLP Network Improvements

- Faster and higher-capacity DLP Network devices. For improved performance, DLP Network now supports running Network devices (Network Controller, Sensor, Interceptor, and ICAP Server) on Dell™ PowerEdge™ R610 hardware with an underlying 64-bit operating system integrated into the DLP Network device software.

  Important: DLP 9.6 is not supported on Dell PowerEdge 2950 appliance.

- IP Mapper can now be configured to retrieve user login/logout information from enVision.
- Allow per policy configuration to notify webmail sender when a sensitive email is detected.

Additional Web Browser Support

- **Enterprise Manager:** Mozilla Firefox versions 13 to 18 are now supported for use with Enterprise Manager.
- **DLP Endpoint:** DLP Endpoint can now monitor end-user web operations in any version of Mozilla Firefox.

Installation Notes

You can upgrade RSA DLP products from version 8.5 and later to DLP 9.6. See the *RSA DLP Upgrade Guide* for more information.

Important: Migration to DLP 9.6 is not supported for Network components on Dell PowerEdge 2950 appliance. For more information, see *RSA DLP 9.6 Upgrade Guide*.

Security Fixes

This section includes the potential security vulnerabilities and issues that have been fixed in RSA DLP 9.6.

- VU#849841: Third-party component, Keyiew Filter SDK, has been upgraded to version 10.16 which has fixes for known security vulnerabilities. For information, see **http://www.kb.cert.org/vuls/id/849841**.
- An SSLv3.0/TLSv1.0 protocol weak CBC mode vulnerability (CVE-2011-3389 aka BEAST attack) in RSA DLP Endpoint Coordinator has been mitigated by usage of unaffected RC4 ciphers.
- Erl.exe in RSA DLP Endpoint Coordinator has been updated to use high strength ciphers by default.

Fixed Issues

This section lists issues fixed since the last major RSA DLP release.

DLP Installation and Upgrade

- Install and upgrade of Enterprise Manager fails if Enterprise Manager database is schema is other than dbo.
- Customization to View DLP Matched Content in an RSA Archer iView was Not Maintained on Upgrade.
- SQL Query error regarding dbo was displayed while upgrading Enterprise Manager.

DLP Enterprise Manager

- An Active Domain user was not able to perform a “Move to Secure” remediation in Enterprise Manager.
- During ICAP webmail replacement, only the active directory/LDAP user was notified of the replacement. The webmail sender was not notified of the replacement.
- DLP Incidents and Events from the database scans were not displayed correctly on the Incident Details and Events Details pages respectively.
- Quarantine failed for filenames including ampersand and for .zip files including .xls files.
- Purge of “Matched Content only” was not supported.
- Import URLs as CSV file feature did not work on the Repository Group configuration page.
- Not able to create a new Reference Dictionary.

DLP Endpoint

- In Windows 7, Endpoint users did not see status message when classification of a large folder or compressed file takes a long time.
- A Copy of sensitive content to a Sandisk drive mounted as an internal laptop drive generated no Events.
- Uploading large file of 150+ Mb crashed Firefox and caused significant delay in other browsers.
- If a user attempt to print a sensitive Microsoft PowerPoint file violates a policy with a match count “Ignore” setting of 0-0, the violation is detected but the event is displayed with a match count of 1 even if the file contains more than one instance of sensitive content. If the PowerPoint print attempt violates a policy with a match count “Ignore” setting of 0-1, no violation is displayed even if the file contains sensitive content.
- On an Endpoint machine running Windows 7, even though the “Show a message to the user if the classification takes more than XX seconds” field is enabled and set to a value such as 10 seconds in the Endpoint group configuration, Endpoint users saw no status message if a copy operation on a large folder or large compressed file involving DLP classification takes longer than the defined value.
- DLP Endpoint was unable to detect violation when sensitive files are transferred to Blackberry device connected to the endpoint machine in MTP mode.
- DLP Endpoint was unable to detect violations using certain Microsoft Word documents containing sensitive content.
- Some DLP Endpoint configuration files were vulnerable to decryption.
- Join service failed to create SSL binding for port 5771 due to other existing IPv6 SSL binding.
- Endpoint agent failed to identify the Group information if SSL is configured for Active Directory.

DLP Network

- The Enterprise Manager does not send email notification to the webmail sender and the company email address when an email containing sensitive content is saved as draft in Hotmail.
- Secure LDAP communication with incorrectly configured certificates broke some DLP policies.
- Unable to attach sensitive files to an email in Outlook Web Application accessed through Google Chrome Browser with Sliverlight plug-in disabled.
- If a violation is detected for a sensitive e-mail with multiline subject text sent using Outlook Web Application, Incident Details and Event Details pages display only partial subject line of the sensitive email.
- After a fresh installation of any Network device, you had to reboot the device after adding it to the DLP Network configuration in Enterprise Manager.
- The Sensor stopped analyzing HTTP POST packets correctly when post size reached or exceeded 64KB and HTTP piggybacking was enabled.
- Network added a UTF-8 BOM before sending data for content analysis, affecting the expected offset for several file types in Enterprise Manager. Highlighting of match content was shifted by one character.
- For e-mails with attachments (Microsoft Word, Excel or PDF files) containing sensitive content and file size less than 125 KB, the matched content is not extracted to the matched content folder.
- Gmail Standard View displays an error message when attempting to send an e-mail with a sensitive file attached to it, and the user is unable to send the e-mail.
- The %attachment_file_name_list% notification variable populated the top 10 attachments list sent out in a Network incident notification email based on the order in which the files were attached, and not in order of priority or severity.

DLP Datacenter

- After the Enterprise Coordinator was uninstalled the Longarm process was not deleted due to which the dependent files were not cleaned up.

- Scan status was set to “Completed” even when scan was incomplete due to Grid Worker being unavailable.
- If the Site Coordinator restarts when a DLP Datacenter scan was in progress, the scan hangs as it failed to recover the incremental scan information.
- During incremental scan Enterprise Manager UI showed Grid Worker as not decommissioned for some workers even though they were decommissioned.
- The communication between DLP Datacenter and the configured active directory was not encrypted.
- Database scans using DLP Datacenter failed when **Selected tables** option is selected on the scan group configuration.
- Matched content was getting displayed with some jumbled characters on Enterprise Manager UI when using Windows 874 character set.
- If communication between Grid Coordinator and Grid Worker was interrupted, different scan results were posted on Enterprise Manager.

Content Analysis

- The <rsahtmlform> element was stripped out while processing form data in DLP Network and DLP Endpoint.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

DLP Installation and Upgrade

Change Button Not Valid for a Previously Installed Component

Problem: If you install Enterprise Manager first and install another component later, the install directory for Enterprise Manager is not displayed on the InstallShield Wizard screen. If you select the **Change** button in order to see the installation directory, an error, Error 2864, occurs and the installer abruptly quits.

Workaround: The **Change** button is not valid for a component that has already been installed. Do not select the **Change** button for a component that has already been installed.

Permissions to Access All Folders Not Granted When You Upgrade

Problem: Permissions to access all of the folders required to run DLP are not granted correctly if you change the Windows service account when you upgrade from previous DLP versions to DLP 9.6.

Workaround: Do not change the service account when upgrading to DLP 9.6.

The Upgrade Fails When Installing Enterprise Manager Under a Custom Folder Named “Enterprise Manager”

Problem: When you install Enterprise Manager under a custom folder named “Enterprise Manager,” the installation path becomes C:\Enterprise Manager\Enterprise Manager. While upgrading, the installer fails to detect the installation path properly, fails to upgrade, and displays the following error:

```
ERROR: Unable to find file 'C:\Enterprise Manager\Enterprise
Manager.bak\webapps\root\WEB-INF\classes\application.properties'.
Upgrade will not be performed.
```

Workaround: Select a name other than “Enterprise Manager” for the custom folder name.

Upgrade Process Aborts When the Enterprise Coordinator Service Is Marked for Delete

Problem: The upgrade process aborts abruptly when the Enterprise Coordinator service is marked for delete.

Workaround: Reboot the Enterprise Coordinator host machine, and run the Repair Installer for Enterprise Coordinator.

When Upgrading from RSA DLP Endpoint 9.0, an Error Message Box May Appear

Problem: When upgrading from DLP Endpoint 9.0, an error message pop-up box may appear on the endpoint machine. The error message states: `The instruction at "XXXX" referenced memory at "XXXXX". The memory could not be "read." Click on OK to terminate the program.`"

Workaround:

1. Select **OK** to close the message box.
2. Ignore the message. The upgrade is not affected.

DLP Enterprise Manager

When You Upgrade to DLP 9.6 from pre-9.5 release, Saved Searches Are Not Migrated

Problem: Any saved Incident and Event searches you created in a pre-9.5 version of DLP are not migrated to DLP 9.6.

Workaround: Before upgrading, document the searches you have saved so that you can recreate them in DLP 9.6.

The Status Always Shows "In Progress" if You Include & in the Agent Name

Problem: If you include "&" in the agent name while generating the pre-configured agent installer in Enterprise Manager, the status always shows "In Progress".

Workaround: The pre-configured agent installer name must not include any of the following characters:

- ampersand (&)
- less-than (<)
- greater-than(>)
- double quote(")
- single-quote (')

Deleting Users and Groups in the Enterprise Manager Takes Longer Than in Earlier Versions of Enterprise Manager

Problem: Deleting users and groups in the Enterprise Manager takes longer than in previous versions of DLP.

The Option to Email Reports to Yourself Does Not Work for LDAP Users

Problem: If you log on to DLP Enterprise Manager as an LDAP user and not with a DLP user logon, the option to email reports to yourself does not work.

On the Scan History File Details Page, the Total Files Count May be More than the Actual Number of Files

Problem: In Enterprise Manager, on the Scan page (**Exchange Scanning History > File Details > Scan**), the total files count may be more than the actual number of files because emails are represented as both .eml and .mail files.

Certain Search Categories Yield Slow Searches on Very Large Lists of Incidents and Events

Problem: Using the protocol/user action, blade, or policy search category results in a slow search through an incident or event list of approximately 1 million items (for example, 10 to 25 seconds on a 693K event list).

On the Policy Page An Error is Displayed When a Valid URL is Entered in the Transmission Attributes Field

Problem: Sometimes when you enter a valid URL in the Transmission Attributes field on the Policy page, Enterprise Manager displays an error message. When you close the error box, the valid URL is really saved to the Enterprise Manager database.

Workaround: To save the policy with the valid URL:

1. Select **OK** on the error dialog box.

   The error dialog box closes.

2. Select **Save** on the Transmission Attributes window.

   The valid URL is saved to the database.

Some DLP Alerts Appear to be Errors But Are Benign

Problem: Some DLP alerts that generate email notifications appear to be errors, but are self-correcting and require no corrective action. Common ones include:

- `EM-003 – Unable to communicate with the database`: Related to a temporary inability to connect Enterprise Manager and the Enterprise Manager Database.
- `EM-005 Unable to communicate with Enterprise Coordinator`: Related to a temporary inability to connect Enterprise Manager and the Enterprise Coordinator.
- `EM-007 – Unable to communicate with Event Loader`: Related to the Event Loader and temporary inability to transmit events among DLP components.
- `NW-010` and `NW-011`: General high and low water mark alerts about low disk space that occur frequently when the operating environment is hovering near the threshold.

Exported Agent Status File Does Not Contain the Same Status Messages as Displayed on the Enterprise Manager

Problem: The exported agent status file does not contain the same status messages as displayed on the Enterprise Manager Agent Group page.

Status Message on the Enterprise Manager Agent Group Page	Status Message in the Exported Agent Status File
Reachable (Not Running) and Status is blank	Not Running
Scanning	Running
Reachable (Not Running) and Status code is 0 and task is not running (harvesting results)	Scan Completed
Completed	Scan Completed
Failed	Scan Failed
Unreachable	Unreachable

DLP Endpoint

Custom Column Settings Return to Default on the Endpoint Agent Management Page

Problem: On the Agent Management page, settings that you change in the “Customize Columns” dialog do not persist after you navigate away from the page.

Workaround: Open and work with the Agent Manage page in multiple tabs or browsers when you need the custom column display to remain the same while you are doing other work in Enterprise Manager.

Endpoint agents are not displayed on Enterprise Manager after upgrading

Problem: After upgrading to RSA DLP, some of the freshly installed Endpoint agents are unable to communicate with the Root Endpoint Coordinator. As a result, these Endpoint agents are not displayed on the Agent Management page.

Workaround: Log on to the Root Endpoint Coordinator machine, and restart the RSA DLP Join Service.

Customized Endpoint Notification Dialog Box Does Not Display Color Correctly

Problem: If you customize the Endpoint Notification, the background color does not display correctly within the dialog box.

Workaround: Use a custom dialogue with a white-colored background.

Data in the "From" and "To" Fields Is Missing from the Incident and Event Details Page for Yahoo Mail Violations

Problem: On the Event and Incident Details page, accessed from the Enterprise Manager console, the "To" and "From" fields located in the Network Transmission Summary area do not contain data for violations detected while using Yahoo mail.

Data in the Email Subject Field Is Missing from the Incident and Event Details Page for Yahoo Mail and Hotmail Violations

Problem: On the Event and Incident Details page, accessed from the Enterprise Manager console, the Email Subject field located in the Transmission Details area does not contain data for violations detected while using Hotmail and Yahoo mail.

"Print to File" Violations During Notepad Use Include the tmp File as the Sensitive File

Problem: A violation detected during a print-to-file operation using a notepad captures as part of the event both the tmp notepad file and the original file used by the operation. This is expected behavior -- the tmp file is the actual text analyzed and where the violation is detected; the original file is considered a source and included in the event for reference, but its content is not included in the match count calculation.

Endpoint Fails to Detect Sensitive Content When Policies Are in Disconnected Mode and Applied to Specific Users

Problem: When you create policies that are applied to specific LDAP users and set to disconnected mode, DLP Endpoint fails to detect sensitive content that is copied to a network share drive.

Workaround: When you create policies that you want to apply specific groups of LDAP users, set the policies to connected mode. Then, create the same policies for all users and set the policies to disconnected mode. You can set connected and disconnected mode in the Enterprise Manager console at the time you create the policy. Disconnected mode means that the policy is in effect when the endpoint machine is disconnected from the organization's network.

In a Clustered Setup, Transfer of Root Endpoint Coordinator Control Fails Due to Certificate Issues

Problem: Root Endpoint Coordinator control does not fail over correctly from an active to a passive Endpoint Coordinator if certificates are not set up on the passive Endpoint Coordinator, and if certificates on the passive Endpoint Coordinator are out of date or unsynchronized. Events and configuration updates cannot be sent to or through the new active Root Endpoint Coordinator.

Workaround: Perform the workaround appropriate to your situation:

- **After certificate renewal and prior to a failover, to avoid the failure when a failover event occurs:**
  - Manually synchronize the certificates on the passive Root Endpoint Controller. For instructions, see the *RSA DLP Maintenance Guide* or the *RSA DLP Troubleshooting Guide*. Proactively synchronizing certificates on the passive Root Endpoint Coordinator allows a failover to happen successfully.

- **After a failover event occurs, and when certificates are out of date or unsynchronized:**
  a. Manually synchronize the certificates on the new active Root Endpoint Controller. For instructions, see the *RSA DLP Maintenance Guide* or the *RSA DLP Troubleshooting Guide*.
  b. In Enterprise Manager, re-add the Endpoint Controller to the DLP Endpoint configuration as the active Root Endpoint Controller. For instructions, see the Enterprise Manager Help.

DLP Network

HTTPS Incidents Marked as HTTP Incidents for Cisco's IronPort S650

Problem: On Cisco's IronPort S650, HTTPS incidents are being marked as HTTP incidents in the incident listings and incident details.

Network Configuration fails for Network Devices on Microsoft Hyper-V Server

Problem: Trying to configure network settings on DLP 9.6 Network devices fail and the user is taken back to the login screen.

Workaround: Perform the following steps:

1. Download **Linux Integration Services Version 3.4 for Hyper-V** ISO and mount it on the DLP Network device.
2. Browse to RHEL directory and install the required RPM files by running the following command:

   ```
   $ rpm -ivh microsoft-hyper-v-rhel63.3.4-1.20120727.x86_64.rpm
   kmod-microsoft-hyper-v-rhel63.3.4-1.20120727.x86_64.rpm
   ```
3. Reboot the Network device.
4. Update network settings.

   Use the following command to edit the **ifcfg-eth0** file:

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   Update the following settings:
   - DEVICE="eth0"
   - BOOTPROTO=none
   - ONBOOT="yes"
   - TYPE="Ethernet"
   - HWADDR=(MAC ADDRESS of device)

     To get the MAC address, enter `ifconfig -a` in a command shell.
5. Save the file and exit.
6. Create a file named **network** under the path **/etc/sysconfig**.
7. Edit the **/etc/sysconfig/network** file and add the following setting:

   ```
   NETWORKING=yes
   ```
8. Save the file and reboot the Network device.
9. Configure network setting.

   For instructions, see the *DLP Network Deployment Guide*.

DLP Datacenter

If Grid Worker machine goes into standby mode during scan, it is unable to continue scanning after resuming from Hibernate or Standby mode.

Problem: While scanning if the grid-worker machine goes into standby mode, after resuming from standby mode, it fails to resume scanning, generate scan report, and decommission agent.

Workaround: Update Windows Power Options settings on the Grid Worker machine to disable it from going to Sleep or Hibernate mode. If the machine was resumed from Hibernate or Standby mode, resume scanning by restarting the Grid Worker Agent Service or machine.

Low-Memory Issues on Grid Workers Caused by Very Large Accumulations of Events

Problem: A very large grid scan, such as a single scan of 50TB of data, takes several days and may stall. If such a scan stalls, event data and related file matches accumulate on the grid workers and can consume a lot of disk space, which may cause low-memory errors and problems on the grid workers.

Workaround: Avoid scanning very large amounts of data in a single grid scan. Consult with RSA Support if needed to come up with alternative scanning options.

SharePoint Online scan appears to have hanged

Problem: While scanning a SharePoint Online repository, Grid Workers wait for a few minutes to get response from the SharePoint Online Webservice before the API call is timed out. In case the API calls time out frequently, the scan may appear to have hanged and time out error messages are logged in the GridWorker log file.

SharePoint incremental scan gives incorrect results.

Problem: In case of incremental scanning of SharePoint Native or SharePoint Online, the scan result may generate duplicate events.

Discovery Agent Scan does not proceed when Agents are configured using LDAPS

Problem: If the LDAPS is configured in Enterprise Manager using the IP address and computers in Discovery Agent scan are configured from the directory, the scan fails.

Workaround: Configure the LDAPs using the FQDN of the LDAP server.

Content Analysis

Fingerprint Crawler Fails on Large .txt Files

Problem: The Fingerprint crawler fails on large .txt files when you select either full or partial path.

Reports

Policy/Content Blade Names that Contain Unicode Characters Do Not Get Displayed Correctly in the CSV File

Problem: When exported from reports, Policy or Content Blade names that contain Unicode characters do not get displayed correctly in the .CSV file when opened in MS Excel or Wordpad.

Workaround: If exported files contain Unicode characters, do the following:

1. Open the .csv file using Notepad.
2. Save the .csv file as a text file (.txt).

3. Import this text file in MS Excel.
4. Save the file as an Excel or .CSV file.

PDF Version of the Compliance Summary Report Consumes Substantial Memory and Slows Enterprise Manager

Problem: Running the Compliance Summary Report to produce PDF output allocates a high amount of memory and can slow Enterprise Manager speed significantly.

Workaround: Run the Compliance Summary Report to produce HTML output only.

Scheduling Incidents or Events Report using “Me” option throws exception when logged in as LDAP user

Problem: An exception is displayed when an LDAP user logged in to Enterprise Manager console tries to schedule Incidents or Events Report and selects “Me” as recipient.

Workaround: Use “Other people” option and specify the full email address.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
RSA Customer Support Information	http://www.emc.com/support/rsa/index.htm
RSA Certified Partner Solution Gallery	https://gallery.emc.com/community/marketplace/rsa

Trademarks