

Release Notes

RSA DLP 9.5 SP1 P1



July 03, 2013

Introduction

This document lists what's new and changed in RSA DLP 9.5 SP1 P1. It includes additional installation information, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

- [Package Contents](#)
 - [Patch Installation](#)
 - [Special Notes](#)
 - [Security Fixes](#)
 - [Fixed Issues](#)
 - [Support and Service](#)
-

Package Contents

The RSA DLP 9.5 SP1 P1 package contains:

- RSA_DLP_Installer_Update_9.5_SP1-P1.exe
 - DLP_Network_9.5_SP1-P1_Upgrade.gpg
-

Patch Installation

Follow the instructions in this section to install the patch.

1. [Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator Upgrade](#)
2. Do the following, in any order:
 - [Network Upgrade](#)
 - [Datacenter Upgrade](#)
 - [Endpoint Upgrade](#)

Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator Upgrade

Important: If the Enterprise Manager, Enterprise Coordinator, and the Root Endpoint Coordinator reside on different machines, perform this procedure on all the machines. You must install the patch on the Enterprise Manager first, and then on the Enterprise Coordinator and the Root Endpoint Coordinator machines.

After installing the patch on the Root Endpoint Coordinator, you must install the patch on all the Endpoint Coordinator machines.

To install RSA DLP 9.5 SP1 P1 on Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator:

1. Copy **RSA DLP Installer Update 9.5-SP1-P1.exe** to the machine hosting the Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.
2. Double-click **RSA DLP Installer Update 9.5-SP1-P1.exe** to start the installation.

3. Follow the instructions on the installation wizard to complete the installation.

Network Upgrade

Perform the following procedure to upgrade the Network Controller and all the Sensors, Interceptors, and ICAP servers.

Important: You must install the patch on the Network Controller first, and then on the Sensors, Interceptors, and ICAP servers, in any order.

Before You Begin

Install the patch on the Enterprise Manager. See [Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator Upgrade](#).

To upgrade the Network Appliances:

1. Copy the **DLP_Network_9.5-SP1-P1_Upgrade.gpg** file to the **/home/tablus** directory.
2. On the Network appliance, go to the DLP Network Main Menu.
3. Select option 4, Check for Updates.
4. Select option 2, Check for updates from the update file on the local system.
5. Follow the remaining prompts as the Network appliance moves through the installation.
After the installation is completed, you will see the updated DLP version number on the tab menu.
6. Repeat steps 1 - 5 on the remaining network appliances.
7. Publish the updated configuration. See [Publish Configuration](#).

Datacenter Upgrade

Perform the following procedure to upgrade the permanent Discovery agents and the grid workers.

Before You Begin

Install the patch on the Enterprise Manager and the Enterprise Coordinator. See [Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator Upgrade](#).

To request Datacenter upgrade and publish updated configuration:

1. On Enterprise Manager, click **Admin > Support > Upgrade Manager**.
The Upgrade Manager appears.
2. Select **Datacenter**, and click **Request Upgrade**.
3. Once the Upgrade Requests table shows the latest version, publish the updated configuration. See [Publish Configuration](#).
The permanent Discovery agents and the grid workers are upgraded during the next scan.

Endpoint Upgrade

Perform the following procedure to upgrade all the Endpoint agents.

Before You Begin

Install the patch on the Enterprise Manager, Root Endpoint Coordinator, and all the Endpoint Coordinators. See [Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator Upgrade](#).

To upgrade the Endpoint agents:

1. In Enterprise Manager, click **Admin > Support > Upgrade Manager**.

The Upgrade Manager appears.

2. Under **Agent Patch Deployment** section, click **Deploy Agent Patch**.

The Endpoint agent upgrade is initiated. You can track the status of the upgrade by viewing the Agent Management page on Enterprise Manager (**Admin > Endpoint > Agent Management**).

Publish Configuration

Note: Perform this procedure only if you are using DLP Datacenter or DLP Network.

1. On Enterprise Manager, click **Admin > Support > Upgrade Manager**.

The Upgrade Manager appears.

2. In the middle of the page, select the product configurations to update by selecting **Network, Datacenter**, or both.

Upgrade Manager

Allow the Enterprise Coordinator to upgrade downstream components for the following:

Datacenter

Request Upgrade

Upgrade Requests:

Product	Upgrade Request Date	Requested Upgrade Version
Datacenter	Mon Jan 14 2013 14:29:08 GMT+0530 (India Standard Time)	9.5.1000

After performing an upgrade installation of Enterprise Manager, you must update the product configurations. Use the checkboxes below to select the products to update, then click "Publish Configuration".

Network

Datacenter

Publish Configuration

3. Click **Publish Configuration**. A dialog appears, explaining that the operation will take place over time.
4. Click **OK** to continue.

The **Update Status** section displays a status and the date and time when Enterprise Manager started deploying updated configuration information to other components.

Wait several minutes before performing additional operations in Enterprise Manager—in particular, avoid changing the configuration and starting scans. This should allow time for configurations to be updated and avoid possible conflicts and problems that may be caused by mismatched configuration information.

Special Notes

After you perform an Enterprise Manager upgrade, you must execute this SQL script to make sure that the right dates are checked when the user lands on 'incidents' or 'events' faceted search. To make the appropriate database changes:

1. Log on to your Enterprise Manager database server and select the Enterprise Manager database.
2. Select **New Query**.
3. Paste the following query into the right-hand-side window:

```
update SE_SEARCH_SETTINGS
set query_properties=
'q=INCIDENT_ASSIGNEE.%24currentUser&q=CREATION_DATE.%5B3600000.%5D&q=CREATION_DATE
.(604800000.172800000%5D&q=CREATION_DATE.(172800000.86400000%5D&q=CREATION_DATE.(8
6400000.3600000%5D' where title = 'Incidents Assigned to Me (Last 7 Days)';
```

In addition to the above query, you can also use the below script to query for events:

```
update SE_SEARCH_SETTINGS
set query_properties =
'q=DATE.%5B3600000.%5D&q=DATE.(604800000.172800000%5D&q=DATE.(172800000.86400000%5
D&q=DATE.(86400000.3600000%5D' where title = 'Events (Last 7 Days)';
```

Important: The PDF converter used to create the release notes may add extra spaces to the query text. If you copy and paste the query from the PDF, spacing problems may occur.

Security Fixes

This section includes the potential security vulnerabilities and issues that have been fixed in RSA DLP 9.5 SP1 P1.

- VU#849841: Third-party component, Keyview 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>.

Fixed Issues

This section lists the issues that have been fixed in this release.

DLP Network

- In some cases, matched content and content blade names are missing in incident or event details, when HTML formatted mails are sent over an Interceptor.
- ICAP splash page displays the Policy Rule ID rather than the Policy ID.

Enterprise Manager

- Scheduled searches with multiple recipients do not reach all users due to the report file being deleted.
- Sender(Network) column when added or deleted impacts the display info of all other columns.
- In some cases, matched content and content blade names are missing in incident or event details, when HTML formatted mails are sent over an Interceptor.
- DLP saved searches are available to all users.
- Non-admin users are unable to remove saved searches.
- The 'Return to the previous page' link on the 'System Error 51' error page redirects to an outdated advanced search format.

Installation

- DLP Endpoint agent encountered an issue while upgrading.
- Enterprise Manager failed to start when upgraded to DLP 9.5 SP1 P1.

Content Analysis

- Enhanced detection of Australian Bank Account Numbers.

Support and Service

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

Copyright © 2013 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.rsa.com/legal/trademarks_list.pdf.