

August 2016

---

## Introduction

This document lists what's new and changed in RSA DLP 9.6.2.6. 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:

- [What's New](#)
  - [Package Contents](#)
  - [Patch Installation](#)
  - [Fixed Issues](#)
  - [Known Issues](#)
  - [Support and Service](#)
- 

## What's New

This section lists what's new and changed in RSA DLP 9.6.2.6.

- Support for User Name Field in Notification Template
- Support for Card Number with the New MasterCard Bin Range
- Support for Reports Deletion

### Support for User Name field in Notification Template

With this release, %user\_name% placeholder can be added to the notification template to display the name of the user whenever an action is performed in violation of policy.

### Support for Card Number with the New MasterCard Bin Range

With this release, card number with the new MasterCard bin range is supported.

### Support to Delete Aged Reports and Index Files

By default you cannot delete aged reports and index files as this feature is turned off. To turn on this feature, edit the `applicationContext-scheduling.xml` and set the parameters `deleteAgedReportFiles` and `deleteAgedSerachIndexFiles` to true.

```
<bean name="agedFilesCleanupJob"
class="org.springframework.scheduling.quartz.JobDetailBean">
    <property name="jobClass"
value="com.tablus.tem.integration.job.AgedFilesCleanupJob" />
    <property name="jobDataAsMap">
        <map>
            <entry key="emConfiguration" value-ref="emconfiguration" />
            <entry key="daysOlder" value="7" />
            <entry key="deleteAgedReportFiles" value="false" /> <!-- set this to
true to delete old report files -->
            <entry key="deleteAgedSearchIndexFiles" value="false" /> <!-- set this
to true to delete old index files -->
        </map>
    </property>
</bean>
```

```
        </map>  
      </property>  
</bean>
```

---

## Package Contents

RSA DLP 9.6.2.6 package contains:

- RSA\_DLP\_Suite\_9.6-SP2-P6.zip
  - RSA DLP Exchange Agent 9.6-SP2-P6.msi
  - RSA DLP Installer Update 9.6-SP2-P6.exe
  - RSA DLP IPMapper 9.6-SP2-P6.msi
- DLP\_Network\_9.6-SP2-P6\_Upgrade.gpg

---

## Patch Installation

Follow the instructions in this section to install the patch.

---

**Important:** You must be running 9.6-SP2 or 9.6-SP2-P1 or 9.6-SP2-P2 or 9.6-SP2-P3 or 9.6-SP2-P4 or 9.6-SP2-P5 before applying the patch.

---

### Steps to install the patch:

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

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

---

**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 9.6.2.6 on Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator:

1. Copy **RSA DLP Installer Update 9.6-SP2-P6.exe** to the machine hosting the Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.
2. Double-click **RSA DLP Installer Update 9.6-SP2-P6.exe** to start the installation.

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

## RSA Data Loss Prevention

**Version:** 9.6.1206 P6  
**EM build number:** 28  
**Installer build number:** 22

▶ [System Information](#)

---

**Notice and Trademarks**  
 Copyright © 2004 -2016 EMC Corporation. All rights reserved. RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, see [www.rsasecurity.com/legal/trademarks\\_list.pdf](http://www.rsasecurity.com/legal/trademarks_list.pdf). EMC is a registered trademark of EMC Corporation. For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com. All other trademarks used herein are the property of their respective owners.

**Disclaimer**  
 RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS". RSA SECURITY, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

**Distribution**  
 Downloading, viewing, copying and printing documents and graphics incorporated in RSA documents and from our Web site is permissible subject to the following conditions: (a) the documents may be used only for personal, informational, non-commercial purposes; and (b) the documents may not be modified or altered in any way. Except where such use constitutes fair use under copyright law, users may not otherwise use, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit or distribute any information from this web site in whole or in part without the express authorization of RSA.

**Third-Party Licenses**  
 This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed at: [Third-Party Licenses](#).

## Upgrade Network Components

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 [Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator](#).

### To upgrade the Network components:

- Copy the **DLP\_Network\_9.6-SP2-P6\_Upgrade.gpg** file to the **/home/tablus** directory.
- On the Network appliance, go to the DLP Network Main Menu.
- Select option 4, Check for Updates.
- Select option 2 -- Check for updates from the update file on the local system.
- 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.
- Reboot the appliance.
  - From the Main Menu on the appliance, select Option 6.
  - Select Option 2.
- Repeat steps 1 - 6 on the remaining network appliances.
- Publish the updated configuration. See [Publish Configuration](#).

Network Status Overview						
Device Name	Device Type	Status	Up Since	Up Time	Software Version	Statistics
<a href="#">10.10.10.10</a>	ICAP Server	Up <a href="#">Details</a>	Mon Jul 25 2016 10:52:42	3 days 3 hours 41 mins	9.6.1206.16	<a href="#">View Statistics</a>
<a href="#">10.10.10.11</a>	Controller	Up <a href="#">Details</a>	Mon Jul 25 2016 10:35:15	3 days 3 hours 59 mins	9.6.1206.16	Not Supported <a href="#">Logs</a>
<a href="#">10.10.10.12</a>	Interceptor	Up <a href="#">Details</a>	Mon Jul 25 2016 14:19:44	3 days 0 hours 14 mins	9.6.1206.16	<a href="#">View Statistics</a>
<a href="#">10.10.10.13</a>	Sensor	Up <a href="#">Details</a>	Mon Jul 25 2016 10:48:50	3 days 3 hours 45 mins	9.6.1206.16	<a href="#">View Statistics</a>

## Upgrade Datacenter Components

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 [Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator](#).

### 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.

The screenshot displays the 'Endpoint Status Overview' dashboard. At the top, it shows the 'Root Endpoint Coordinator' status as 'Up' with a green checkmark. Below this, there are three columns for 'Endpoint Coordinators', 'Endpoint Groups', and 'Endpoint Agents', each with a count of '1'. To the right, 'Certificate Statistics' are shown: Issued (1 green checkmark, 0 red X) and Renewed (0 green checkmark, 0 red X). A 'Reset' button is also present. The 'Datacenter Status Overview' section shows the 'Enterprise Coordinator' as 'Up' with version 9.6.1206.11. Below this is a table with columns for 'Site', 'Status', 'Agent Groups' (Total, Agent Deployments in Progress), and 'Grid Groups' (Total, Scans in Progress). The table shows one site, 'SITE\_125', with a status of 'Up' and 1 total agent group, 0 in progress, 1 total grid group, and 0 scans in progress. At the bottom, the 'Enterprise Manager' section lists logs: Application Log, System Alerts Log, and Event Loader Log.

## Upgrade Endpoint Agents

Perform the following procedure to upgrade all the Endpoint agents.

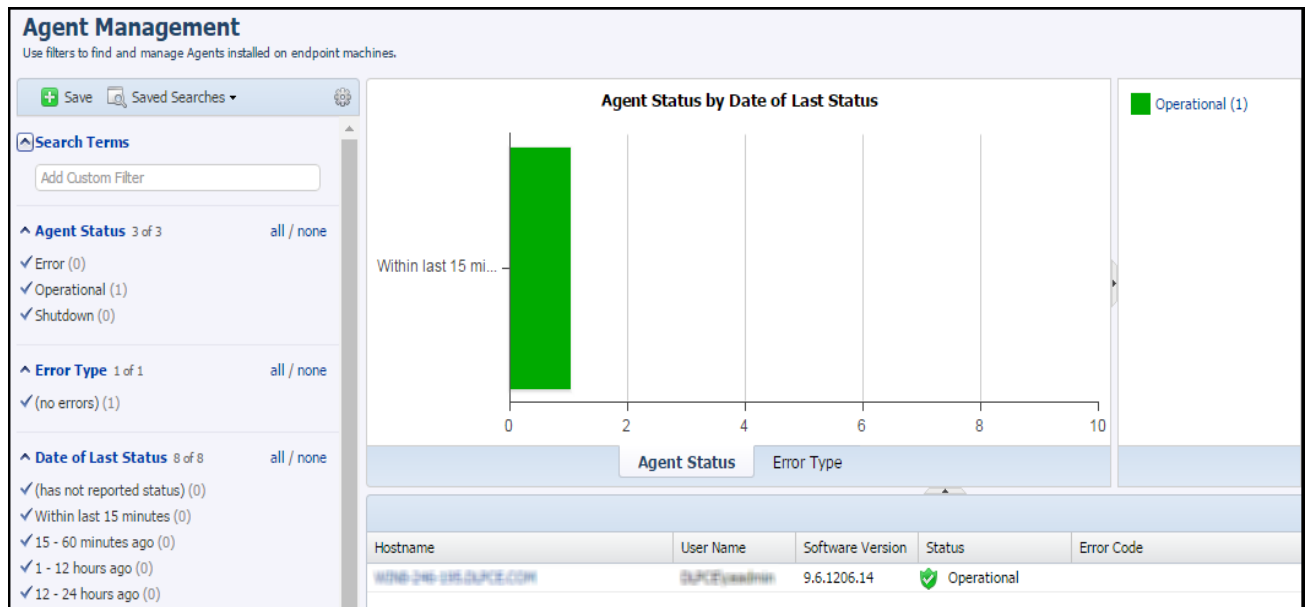
### Before You Begin

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

### To upgrade the Endpoint agents:

1. In Enterprise Manager, click **Admin > Support > Upgrade Manager**.  
The Upgrade Manager page appears.
2. Under the **Agent Patch Deployment** section, click **Deploy Agent Patch**.

All the existing endpoint agents are automatically upgraded.



## Publish Configuration

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.

The screenshot shows the 'Upgrade Manager' interface. It includes a 'Request Upgrade' button, a table of 'Upgrade Requests', and checkboxes for 'Network' and 'Datacenter' to be updated. Below these are 'Publish Configuration' and 'Update Status' sections.

Product	Upgrade Request Date	Requested Upgrade Version
Datacenter	Wed Jun 01 2016 17:40:41 GMT+0530 (India Standard Time)	9.6.1201
Datacenter	Thu Jun 02 2016 13:00:10 GMT+0530 (India Standard Time)	9.6.1202
Datacenter	Thu Jun 02 2016 16:42:28 GMT+0530 (India Standard Time)	9.6.1203
Datacenter	Fri Jul 15 2016 12:50:31 GMT+0530 (India Standard Time)	9.6.1206

Device Name	Device Type	Status	Update Date
10.30.240.44	Network Controller	Successfully Updated	Tue Jul 26 2016 14:54:05 GMT+0530 (India Standard Time)
10.30.240.124	Enterprise Coordinator	Successfully Updated	Tue Jul 26 2016 14:54:05 GMT+0530 (India Standard Time)

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.

---

## Fixed Issues

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

### DLP Endpoint

- Unable to detect violations, when Adobe Save As PDF option is selected and the file is copied to network share.
- Unable to classify the files when multiple files are attached in the Hotmail.
- Unable to classify files when multiple files are attached in the Yahoo Mail.
- Endpoint unable to detect violations when you select save as Adobe PDF in Microsoft Office application.

### DLP Enterprise Manager

- Unauthorized error is displayed when the Content Blade Manager page is accessed.
- Policy action error is not applied based on the severity level.

### DLP Network

- IP Mapper consumes 100 percentage CPU on Win 2012.
- Parsing is displayed while processing HTTP traffic on ICAP.
- Policy Action based on the File Extension is not correct.

---

## Known Issues

### Network Controller `javax.net.ssl.SSLException` unable to communicate with EM

**Problem:** The Network Controller is unable to send event.zip to EM due to an error message seen on Network Controller `messages.log` file.

**Workaround:** If Network Controller is unable to communicate with EM, do the following:

1. Logon to Network Controller as a root user and execute the following commands:  

```
chmod o-r /usr/java/latest/lib/security/java_nonfips.security
chmod o-r /usr/java/latest/lib/security/java_fips.security
```
2. Restart the Network Controller services.

### Username files are not populated on controller

**Problem:** Username files are not populated on Controller when Enterprise Manager is on Win 2012.

**Workaround:** Install Enterprise Manager on Win 2008.

---

## Support and Service

---

RSA SecurCare Online	<a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a>
Customer Support Information	<a href="http://www.emc.com/support/rsa/index.htm">http://www.emc.com/support/rsa/index.htm</a>
RSA Solution Gallery	<a href="https://gallery.emc.com/community/marketplace/rsa">https://gallery.emc.com/community/marketplace/rsa</a>

---

Copyright © 2016 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.emc.com/legal/emc-corporation-trademarks.htm](http://www.emc.com/legal/emc-corporation-trademarks.htm).