Release Notes
RSA DLP 9.6.2.6

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

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>
```

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

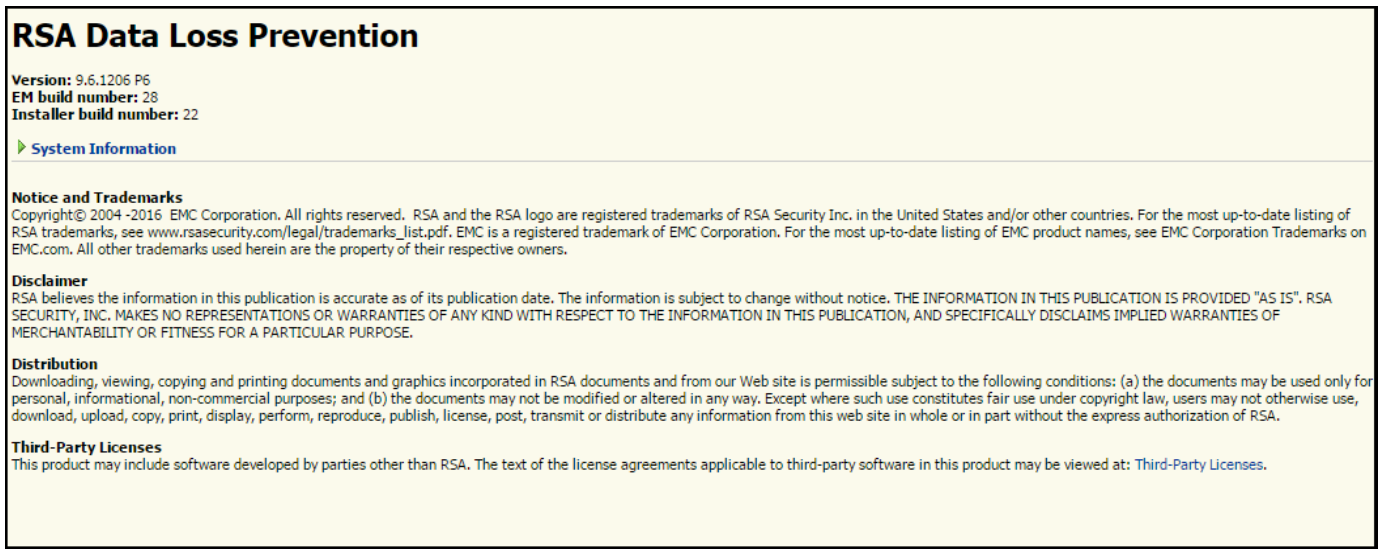
Important: If the Enterprise Manager, Enterprise Coordinator, and the Root Endpoint Coordinator reside on different machines, perform this procedure on all the machines. You must install the patch on the Enterprise Manager first, and then on the Enterprise Coordinator and the Root Endpoint Coordinator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

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



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.

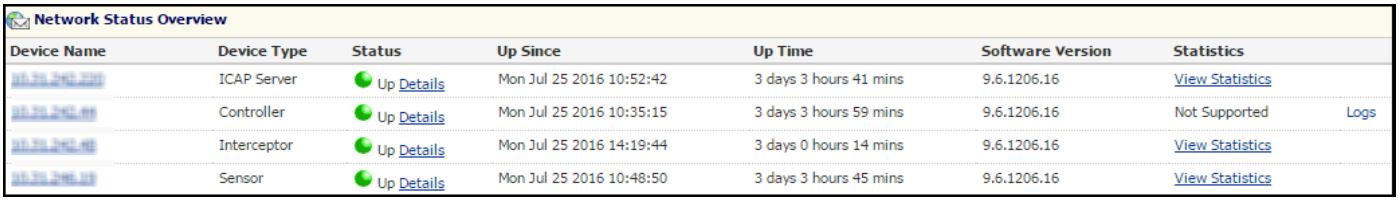
Before You Begin

- Install the patch on the Enterprise Manager. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

To upgrade the Network components:

1. Copy the **DLP_Network_9.6-SP2-P6_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. Reboot the appliance.
   a. From the Main Menu on the appliance, select Option 6.
   b. Select Option 2.
7. Repeat steps 1 - 6 on the remaining network appliances.
8. Publish the updated configuration. See Publish Configuration.



Upgrade Datacenter Components

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

Before You Begin

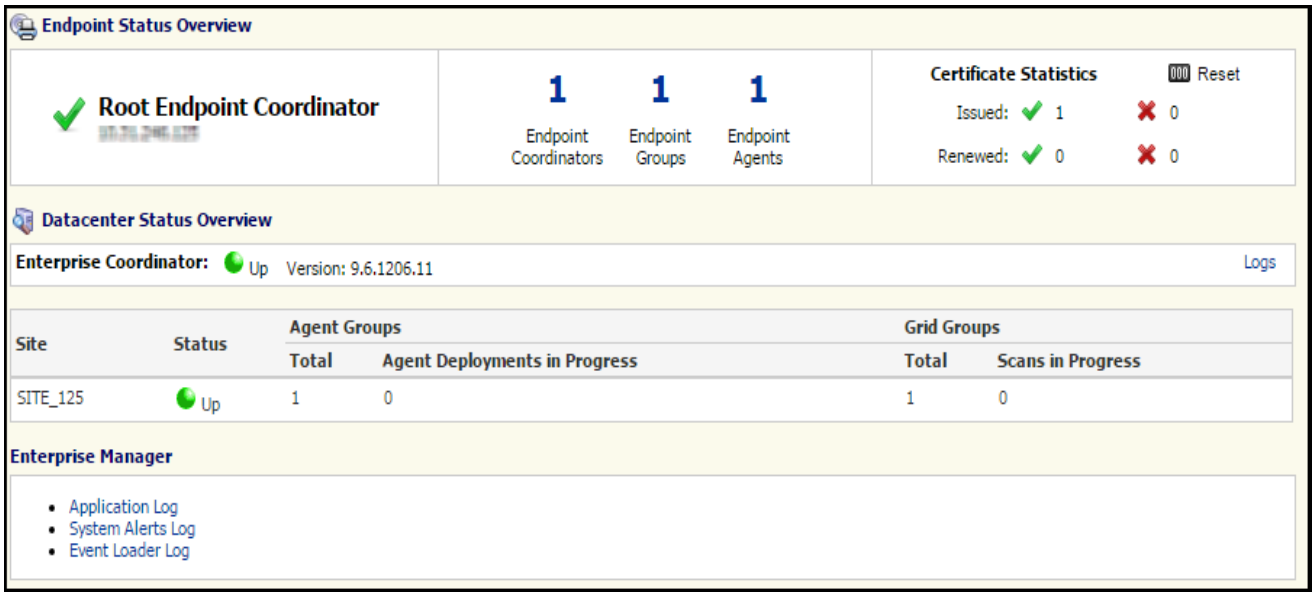
- Install the patch on the Enterprise Manager and the Enterprise Coordinator. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

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.



Upgrade Endpoint Agents

Perform the following procedure to upgrade all the Endpoint agents.

Before You Begin

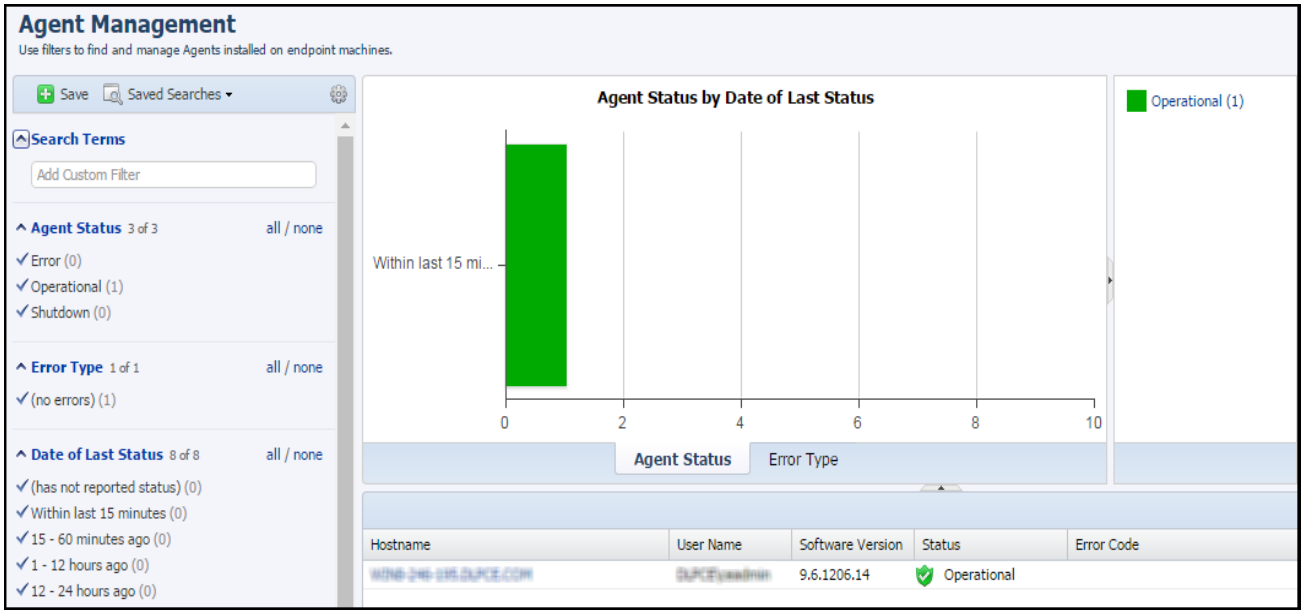
- Install the patch on the Enterprise Manager, Root Endpoint Coordinator, and all the Endpoint Coordinators. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

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.



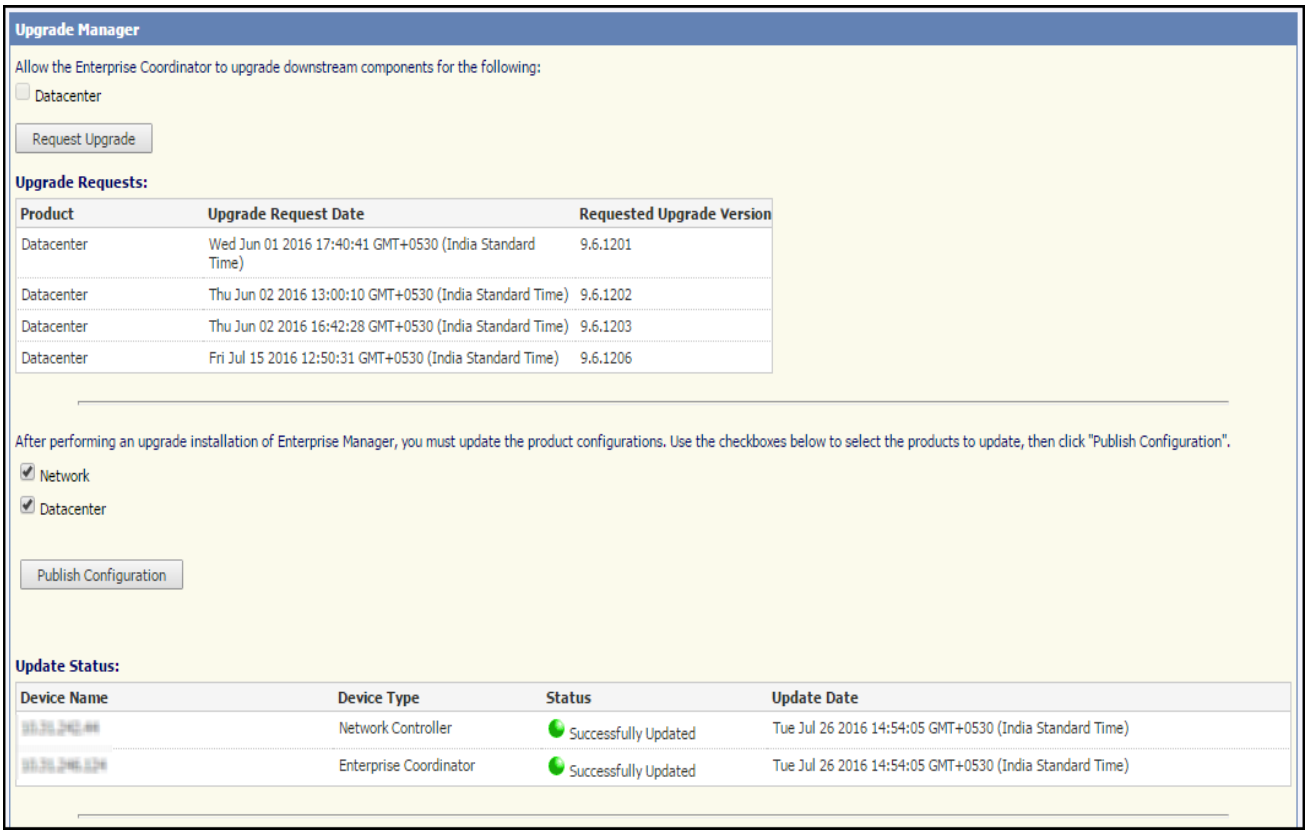
Publish Configuration

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.



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 consumes100 percentage CPU on Win 2012.
- Parsing is displayed while processing HTTP traffic on ICAP.
- Policy Action based on the File Extenstion 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	https://knowledge.rsasecurity.com
Customer Support Information	http://www.emc.com/support/rsa/index.htm
RSA Solution Gallery	https://gallery.emc.com/community/marketplace/rsa

Trademarks