Release Notes
RSA DLP 9.6 SP3

February, 2017

Introduction

This document lists what's new and changed in RSA DLP 9.6 SP3. 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:

Note: RSA DLP 9.6.3 is supported on Internet Explorer version 8 to 11, Mozilla Firefox version 13 to 50 and Microsoft Edge browser.

What's New

This section lists what's new and changed in RSA DLP 9.6 SP3.

Support for Windows 10 Operating System

With this release, RSA DLP Endpoint and DLP Data Center are supported on Windows 10 Operating System.

Support for Microsoft Office 2016

With this release, RSA DLP supports Microsoft Office 2016.

Support for Microsoft SQL 2014

With this release, RSA DLP supports Microsoft SQL 2014.

Support for Microsoft .NET Framework 4.5.2

With this release, RSA DLP Endpoint supports Microsoft .NET Framework 4.5.2 or above.

Support for Microsoft Edge Browser on Windows 10 Operating System

With this release, RSA DLP Endpoint supports and monitors Microsoft Edge browser on Windows 10 Operating System.

To enable Microsoft Edge Browser monitoring, perform the following:

1. On the **Enterprise Manager** page, click **Admin**.
2. In the **Endpoints** drop-down, click **Endpoint Groups**.
3. Click the required group. For example, **Default**.
4. In the **Endpoint Group - New/Edit** page, click **Edit**.
5. Click **Tech Support Only**.
6. In the **Include Applications** field, add the following applications:

   ```
   MicrosoftEdge.exe
   MicrosoftEdgeCP.exe
   ```

7. In the **Override Configuration** field, add the below tag:

   ```
   <Advanced><MonitorEdgeBrowser>true</MonitorEdgeBrowser></Advanced>
   ```

8. Click **Save**.

Package Contents

RSA DLP 9.6 SP3 package contains:

- RSA_DLP_Suite_9.6-SP3.zip
  - RSA DLP Exchange Agent 9.6-SP3.msi
  - RSA DLP Installer Update 9.6-SP3.exe
  - RSA DLP IPMapper 9.6-SP3.msi
- DLP_Network_9.6-SP3_Upgrade.gpg

Service Pack Installation

Follow the instructions in this section to install the service pack.

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 or 9.6-SP2-P6 before applying the service pack.

Steps to install the service pack:

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 service pack on the Enterprise Manager first, and then on the Enterprise Coordinator and the Root Endpoint Coordinator machines.

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

To install RSA DLP 9.6 SP3 on Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator:

1. Copy **RSA DLP Installer Update 9.6-SP3.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-SP3.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 service pack on the Network Controller first, and then on the Sensors, Interceptors, and ICAP servers, in any order.

Before You Begin

- Install the service pack 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-SP3_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

Note: For information on deploying DLP Datacenter components using custom deployment, see "Using Custom Credentials to Install DLP Datacenter Components" on page 6.

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

Before You Begin

- Install the service pack 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 service pack 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** > **Endpoint** > **Generate Agent Installer**.

   The Agent Installer page appears.

2. Under the **Agent Installer** section, do the following:

   a. In the **Name** field, enter a name for the agent installer.

   b. (Optional). Include the policy and configuration files in the agent installer. Select Include Policy and Configuration Files.

   c. Click **Generate Installer**.

   Enterprise Manager generates the agent installer and saves it in the Event and Report indexing folder. The default location is:
   C:\RSA\agent\installer

3. Copy the generated installer to the Endpoint Agent machine.

4. Double-click the installer file to start the installation wizard. Click **Run**, if a security warning appears.

   Important: You must launch the installer as an administrator.

   The installation wizard opens.

   Note: You can also upgrade the Endpoint Agent using third-party tools such as Microsoft System Center Configuration Manager (SCCM). For more information, see RSA technical note *Using SCCM to Install DLP Endpoint Agents*.

5. Read the Welcome text, then click **Next**.

   The Destination Folder screen appears.

6. Accept the default installation directory shown, or click **Change** and navigate to the directory where you want the agent to be installed.

7. Click **Next**.

   The Root Endpoint Coordinator Configuration screen appears.

8. Do the following:

   a. Enter the FQDN, Hostname, or IP address of the Root Endpoint Coordinator.

   b. Enter the **Agent Authorization Key**.

   The Authorization key can be generated using the Enterprise Manager console. For more information, see *RSA DLP 9.6 Upgrade Guide*.

   c. Click **Next**.

   The Ready to Install the Application screen appears.

9. Click **Install** to begin installing the agent.

During the installation, the Installing RSA DLP Endpoint Agent screen displays progress. When installation completes, the Successful Installation screen appears.

10. Click **Finish** to close the Installation Wizard.

Note: Microsoft .NET Framework 4.5.2 or above is required to install RSA DLP 9.6.SP3 Endpoint Agent. Make sure that the Microsoft .NET Framework version is supported on the Host Operating System before you proceed with the installation. For more information, see **https://msdn.microsoft.com/en-us/library/8z6watww(v=vs.110).aspx**.

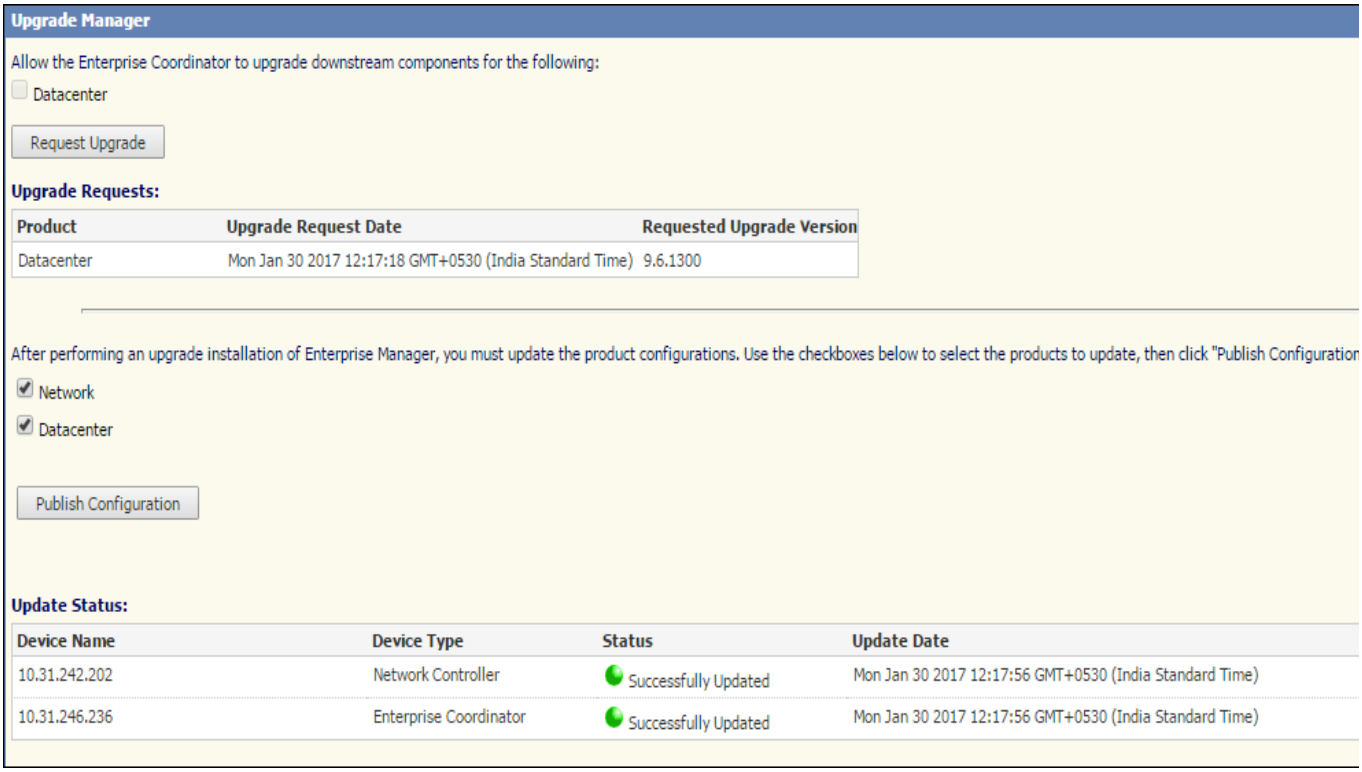
Publish Configuration

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.



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.

Using Custom Credentials to Install DLP Datacenter Components

For hardened environments, where non-system account is required to run specific DLP services, a non-system account can be used to run the services required.

Important: Automatic bootstrapping of downstream components is not supported. You will have to manually install all downstream components like Site Coordinators, grid workers, and discovery agents. Stop all Site Coordinator services before upgrading Enterprise Coordinator.

Following Datacenter components can be provided with custom credentials during installation:

- Enterprise Coordinator
- Site Coordinators
- Grid Workers
- Discovery Agents

Pre-Installation Tasks

Before using the procedures, make sure that you have completed the following steps.

Note: The entire Group Policy Management must be done on a Domain controller machine.

1. Create a custom User Group in Active Directory. For example, DLPUsers.
2. Specify GPO policies to the group (DLPUsers).

Note: Following is a sample procedure to set GPO policies. Contact your Active Directory administrator to make these changes.

   a. Open Group Policy Manager and add a new domain policy GPO.
   b. Update the GPO scope to include the machines targeted for Datacenter components.
   c. Edit the newly created GPO.
   d. The Group Policy Management Editor opens.
   e. Browse to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.
   f. Add the group (DLPUsers) to the following policies:
      – Debug programs
      – Log on as a service
      – Replace a process level token
      – Back up files and directories
      – Restore files and directories
      – Impersonate a client after authentication

Note: This setting will override the default GPO policy settings. If you need the default settings, make sure to include them while making the changes.

   g. Link the GPO to the domain and enforce it.
3. Create a User and add the user to the user group (DLPUsers). You can add an existing user to the DLPUsers group.
4. Update the GPO policies on all the devices targeted for installing DLP Datacenter components.

Note: The **Automatically Upgrade Components** checkbox must be de-selected from the Enterprise Coordinator configuration page.

5. Stop all Site Coordinator services.

Manually Install Site Coordinators or Grid Workers

Use the following procedure to use custom credentials to install Site Coordinators or Grid Workers.

Before You Begin:

- Configure Enterprise Coordinator. For instructions, see “Initially Configuring the Enterprise Coordinator” section in the Datacenter Deployment Guide.
- Get GPO/Push Site Password from the Enterprise Manager console.

  If you are installing first Site Coordinator you can get the GPO/Push Site Password by going to the add Site Coordinator page.

To manually install Site Coordinator or Grid Worker:

1. Copy the Agent.msi from Enterprise Coordinator machine to the target machine.

   The installer is available in *`EC_INSTALL_DIR/Discovery/EnterpriseCoordinator/Dependencies`* directory.
2. Double-click the Agent.msi file to start the installation wizard.

   The installation wizard opens.

   Important: You must launch the installer as an administrator.
3. Read the Welcome text, then click **Next**.

   The Destination Folder screen appears.
4. Do the following:
   a. Accept the default installation directory shown, or click **Change** and navigate to the directory where you want the agent to be installed.
   b. Enter the Port number to be used by Site Coordinator or Grid Worker.
   c. Select the **Use custom credentials for DLP Datacenter components** checkbox to specify credentials for Site Coordinator and Grid Worker.
   d. Specify the GPO password.
   e. Click **Next**.
   The DLP Datacenter Service Credentials screen appears.
5. Do the following:
   a. Enter the domain name for the Site Coordinator and Grid Worker machine.
   b. Enter the group name to be used for the Site Coordinator and Grid Worker service.
   c. Enter the user name to be used for the Site Coordinator and Grid Worker service. The user must be part of the specified group.
   d. Enter the password for the specified user name.
   e. Click **Next**.

   The installer tries to verify the entered values. on successful verification, Ready to Install screen appears.
6. Click **Install** to begin installation.

   On successful installation, the Wizard Completed screen appears.
7. Click **Finish** to close the installation wizard.

After installing the Datacenter components with custom credentials, you can configure them in the Enterprise Manager console.

Security Fixes

- Openssh security update. For information, see security advisory RHSA-2016:0466-1. The Openssh security update (CVE-2015-5600, CVE-2016-3115) affects only the RSA DLP Network component.
- Java is upgraded from version 7 to 8 to address multiple security issues.
- Madshi library is upgraded from version 3.1.10 to 3.1.12 to address PAGE_EXECUTE_READWRITE issues.

Fixed Issues

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

DLP Endpoint

- Endpoint fails to detect violation when a file is uploaded to Hotmail, Gmail, or Yahoo Mail using Internet Explorer.

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.

Unable to capture violation during print functionality in the Microsoft Edge browser

Problem: Unable to capture violation during print functionality in the Microsoft Edge browser.

Workaround: None.

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