RSA® Authentication Manager 8.5

Patch 1 Security Update 1 Readme

December 2020

Prerequisite Release:
RSA Authentication Manager 8.5

Contents

Before Installing Patch 1 Security Update 1

Note: All RSA Authentication Manager 8.5 patch releases and security updates are cumulative. You only need to apply the most recent patch or security update to obtain all of the software fixes and updates that are included in the previous patches for version 8.5.

Before installing this update, review the following guidelines:

- You must upgrade RSA Authentication Manager to version 8.5 before installing this update. For more information, see "Upgrading RSA Authentication Manager" on RSA Link at https://community.rsa.com/docs/DOC-100620.
- You must have at least 4 GB of free disk space to apply this update.
- You must apply this update to the primary and all replica instances in your RSA Authentication Manager 8.5 deployment. Make sure you apply the update to the primary instance before applying the update to the replica instances.
- Before using the Security Console wizard to connect Authentication Manager directly to the Cloud Authentication Service, you must upgrade your primary instance and all replica instances.
- If you have a replicated environment, all replica instances must be running and replicating successfully before you apply the update to the primary or replica instances. On the primary instance, the replication status displays "Internal Replication Error" or another error message until all replica instances have been upgraded or patched.
- SSH clients and SCP clients can no longer connect to the appliance with weaker algorithms, for example, MD5 and 96-bit MAC algorithms. It may be necessary to upgrade your SSH and SCP clients to more recent versions that can handle more restrictive SSH algorithms.
- A security update for the web-tier server (available *here*) is also available. See the web-tier server *Readme* for information on the updates to the web-tier server.

Installing This Security Update

The RSA Authentication Manager 8.5 Patch 1 Security Update 1 ZIP file (**am-update-8.5.0.1.1.zip**) contains the RSA Authentication Manager 8.5 Patch 1 Security Update 1 ISO file, **am-update-8.5.0.1.1.iso**, that is used to apply the update to Authentication Manager.

You can apply an update through your web browser, or you can store patches in an NFS share, a shared folder on Windows, a DVD/CD, or an ISO image on your local machine.

The overall steps to install this patch are as follows:

- Specify a Product Update Location
- Scan for Product Updates
- Apply Product Update

Specify a Product Update Location

To specify a product update location, or to edit a previously specified location, perform the following procedure. This will allow RSA Authentication Manager 8.5 to locate patches.

If you have already specified a location, see Scan for Product Updates on page 3.

Before You Begin

To scan for updates on an RSA-supplied DVD or CD, do the following:

- On a hardware appliance, use the DVD/CD drive or mount an ISO image.
- On a virtual appliance, you must configure the virtual appliance to mount a DVD/CD or an ISO image. See the Operations Console Help topic "VMware DVD/CD or ISO Image Mounting Guidelines."

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. On the Update & Rollback page, the default update source is your local browser. To change that setting, click **Configure Update Source**.
3. On the Configure Update Sources page, specify a location for updates.
   - To apply a specific update, select **Use your web browser to upload an update**. You do not need to scan for updates.
   - To scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: **192.168.1.2:/updates**
   - To scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.
     - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: **\\192.168.1.2\updates**
     - (Optional) In the **Windows Username** field, enter a username.
     - (Optional) In the **Windows Password** field, enter a password only if it is required by

your Windows share configuration.

- To scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.

4. To test the NFS or Windows share directory settings, click **Test Connection**.

   A message indicates whether the configured shared directory is available to the primary or replica instance.

5. Click **Save**.

Next Steps

Do one of the following:

- If you configured your local web browser as the method to apply an update, see Apply Product Update on page 4.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, see Scan for Product Updates on page 3.

Scan for Product Updates

If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, you can scan to locate and review a list of available product updates. If you want to apply an update through your local web browser, then you do not need to scan for updates.

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. Click **Scan for Updates**.

   The system displays the progress of the scan on the **Basic Status View** tab. You can view more detailed information on the **Advanced Status View** tab.

3. Click **Done** to return to the Update & Rollback page.
4. In the **Applied Updates** section, click **Download Detailed History Log** for a complete update history.

   The **Applied Updates** section displays the updates applied to the instance. This section includes the update version numbers, the time and date that each update was applied, and which administrator applied the update.

Note: After you scan for updates, the new list displays for 24 hours. Logging out of the Operations Console does not remove the list from the system cache. If you restart the Operations Console, download additional updates, or change the product update locations, you must perform another scan to see the most current list.

Next Steps

Apply the update to the RSA Authentication Manager deployment.

Apply Product Update

Apply the update to the primary instance first, and then to each replica instance.

Before You Begin

- Restart the Authentication Manager appliance where you are installing the update.
- Ensure that port 8443/TCP is open for https traffic.

  Access to this port is required for real-time status messages when applying Authentication Manager patches and service packs.

  During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete.

  If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.
- Specify a Product Update Location, as described on page 2.
- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, Scan for Product Updates, as described on page 3.
- In a replicated deployment, all replica instances must be running and replicating successfully before you apply the update to the primary or replica instances. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

  After upgrading the primary instance, the replication status displays “Internal Replication Error” or another error message until all replica instances have been upgraded or patched.
- Download and unzip the patch from RSA Link to a location that the primary or replica instance can access.
- If you localized Authentication Manager, make sure that you have a copy of your localized JAR files. Some Authentication Manager updates include Java Development Kit (JDK) upgrades. JDK upgrades might overwrite common components in the Authentication Manager installation directory.

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. RSA recommends that you apply the most recent update. Do one of the following, depending on your configuration:
   - To apply an update through your local web browser, do the following:
     a. Click **Upload & Apply Update**. Because browser uploads require additional processing, the Upload & Apply window may open slowly.
     b. Under **Update Location**, click **Browse** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.
     c. Click **Upload**.

- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:

  a. Click **Scan for Updates**. **Available Updates** displays all of the updates that can be applied.

  b. Next to the update to apply, click **Apply Update**.

3. Check the update details, enter the password for the User ID **rsaadmin**, and then click **Apply**.

   As the update process begins, the following occurs:

   - In the **Upload & Apply** window, the **Basic Status View** tab shows the progress of the update preparation process. More detailed information appears on the **Advanced Status View** tab.
   - When the update preparation is complete, the **Upload & Apply** window closes, and a new browser window opens in which to complete the update process.

     Note: When applying the update, a certificate warning might appear. In this case, you can safely click **Continue to this website** to proceed with the update.

   - In the new browser window, the Update Installer applies the update. The **Basic Status View** tab shows the progress of the update as it is applied. More detailed information appears on the **Advanced Status View** tab.

4. When the update is complete, click **Done**.

   The Operations Console opens to the Log On page.

   Applying the patch results in the following:

   - In the Operations Console, on the Update & Rollback page, the update appears in the **Applied Updates** section. To save the high-level update history, click **Download Detailed History Log**.
   - In the Security Console, the Software Version Information page is updated with the patch number.

Next Steps

- You can download a detailed log file containing the information that was displayed on the **Advanced Status View** tab. The file is named **update-*version-timestamp*.log**, where *version* is the update version number and *timestamp* is the time that the update completed. For instructions, see the Operations Console Help topic "Download Troubleshooting Files."
- After you have upgraded the primary instance and all of the replica instances, verify that replication and RADIUS replication is functioning correctly on the primary instance and each replica instance.
- A security update for the web-tier server (available *here*) is also available. See the web-tier server *Readme* for information on the updates to the web-tier server.

Rolling Back This Update

When you roll back an update, you remove the update and all of the fixes included in the update. You can only remove the last update that was applied to Authentication Manager.

Note: Certain component updates and configuration changes related to the operating system, RADIUS, AppServer, Java, or the internal database cannot be automatically reversed by rolling back an update.

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.

   Under **Applied Updates**, a list of updates displays with the following information:

   - **Version**. The version of the update. To see the current version of the Authentication Manager instance, refer to the top of the Update & Rollback page.
   - **Updated on**. When the update was applied. If a log file is available, you can click **Download log** to save and read information about the update process.
   - **Updated by**. The user who applied the update.
   - **Action**. Displays the **Roll Back Update** button or the message "Cannot be rolled back."

2. To roll back the last update that was applied, click **Roll Back Update**. Only a reversible update can be rolled back.
3. Enter the password for the User ID **rsaadmin**, and then click **Rollback**.

   As the patch rollback process begins, the following occurs:

   - In the **Confirm Rollback Update** window, the **Basic Status View** tab shows the progress of the rollback preparation process. More detailed information appears on the **Advanced Status View** tab.
   - When the update preparation is complete, the **Confirm Rollback Update** window closes, and a new browser window opens in which to complete the rollback process.
   - In the new browser window, the Update Installer rolls back the update. The **Basic Status View** tab shows the progress of the update as it is rolled back. More detailed information appears on the **Advanced Status View** tab.

4. When the rollback is complete, click **Done**.

   The Operations Console opens to the Log On page.

What is New in Patch 1 Security Update 1

Patch 1 Security Update 1 includes all new features and enhancements introduced in Patch 1. In addition, Security Update 1 updates RSA Authentication Manager components to prevent potential security vulnerabilities.

Updated RSA Authentication Manager Components

To address **AM-39894**, Patch 1 Security Update 1 provides new versions of the Oracle WebLogic and Java components used by RSA Authentication Manager 8.5. These updates prevent the potential security vulnerabilities that were announced by Oracle as part of the *Oracle Critical Patch Update Advisory (CPU) for October 2020*:

- Oracle WebLogic

  CVE-2019-17267, CVE-2020-14841, CVE-2020-14825, CVE-2020-14859, CVE-2020-14820, CVE-2020-14757

- Oracle Java

  CVE-2020-14792, CVE-2020-14781, CVE-2020-14782, CVE-2020-14797, CVE-2020-14779

The update also resolves issue in components and features that are not used by Authentication Manager, such as the WebLogic Console (CVE-2020-14883, CVE-2020-14882, CVE-2020-11022 and CVE-2020-14750).

New Features and Enhancements in the Earlier Cumulative Patch 1

RSA Authentication Manager 8.5 includes all new features and enhancements introduced in the cumulative Patch 13 for version 8.4.

Patch 1 for version 8.5 includes the following new feature introduced in Patch 14 for version 8.4:

Administrative Roles Have Separate Permissions to Unlock an Account or Enable and Disable Accounts

To address **AM-39487**, Patch 1 changes the permissions that you can select when you add or edit an administrative role. On the General Permissions tab, the **Unlock Accounts** checkbox and the **Enable/Disable Accounts** checkbox replace the combined **Enable/Disable/Unlock Accounts** checkbox. When you add or edit a predefined or custom administrative role, you can give the role permission to unlock accounts and you can give the role permission to enable and disable accounts.

When you apply Patch 1, both new permissions are enabled for any predefined or custom administrative roles that have the **Enable/Disable/Unlock Accounts** checkbox selected.

If you remove Patch 1, the **Enable/Disable/Unlock Accounts** checkbox is selected for administrative roles that have the **Unlock Accounts** checkbox enabled. If only the **Enable/Disable Account** checkbox is selected, then the **Enable/Disable/Unlock Accounts** checkbox is not selected.

When you restore Patch 1 from a backup created with an earlier version of Authentication Manager, the **Enable/Disable Accounts** checkbox is not selected. The **Unlock Accounts** checkbox is selected if the **Enable/Disable/Unlock Accounts** checkbox is selected in the backup file. For each administrative role that requires permission to enable and disable accounts, select the **Enable/Disable Accounts** checkbox.

Defects Fixed in This Update

Version 8.5 Patch 1 Security Update 1

RSA Authentication Manager 8.5 Patch 1 Security Update 1 includes all fixes introduced in all version 8.5 and version 8.4 patches. In addition, Security Update 1 addresses **AM-39894**. See Updated RSA Authentication Manager Components on page 7.

Version 8.5 Patch 1

RSA Authentication Manager 8.5 Patch 1 includes all fixes introduced in RSA Authentication Manager 8.4 Patch 14 and earlier patches. In addition, Patch 1 contains fixes for the following issues:

AM-39706. Updated the version of Oracle WebLogic used by Authentication Manager to prevent potential security vulnerabilities.

AM-39690. Fixed an issue that caused backups to freeze while backing up RSA RADIUS. This situation sometimes occurred after Back Up Now in the Operations Console was used to perform dozens of continuous manual backups at intervals of an hour or less.

AM-39675. Fixed the MinTokenLife option for the AMBA **Replace Token Automatic** (REPTA) command.

AM-39530. Added information about the Dell PowerEdge R240 to the *RSA SecurID Hardware Component Updates* page on RSA Link.

AM-39514. Corrected a field that was not localized into Japanese in the Self-Service Console.

AM-39513. Fixed an issue in which on-demand authentication was not enabled for a customer who was imported into a new deployment.

AM-39512. Fixed the “Administrators of a Security Domain” report to display the correct administrative scope.

AM-39489. Fixed an issue that caused email notifications to be sent based upon the last saved workflow policy, instead of the workflow policy for the user domain

AM-39488. When Authentication Manager is configured to not require a PIN for any tokens, Authenticate Tokencode users are no longer prompted to create a PIN.

AM-39486. Fixed an issue that caused a memory leak while backing up data

AM-39484. Updated the system log to provide more information on which Active Directory connection is being used. The system log now reports when the Directory URL (primary AD connection) fails and when the primary connection is restored

AM-39469. Can now delete CT-KIP activation codes for deleted users.

AM-39468. Resolved an issue with regenerating the root CA for trusted realms.

AM-39466. Resolved a certificate issue that blocked access to the Identity Router Setup Console.

AM-38418. The patch installer restores the PAM configuration to the auto-generated, default state. This could eliminate unsupported changes to this configuration which might cause problems in the RSA Authentication Manager.

AM-32381, AM-32382, AM-32383, AM-32384. Reject some cross-site scripting attempts as invalid.

Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

December 2020

Intellectual Property Notice

This software contains the intellectual property of RSA or is licensed to RSA from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of RSA.

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, RSA or its affiliates will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. RSA or its affiliates may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to RSA Legal, 174 Middlesex Turnpike, Bedford, MA 01730, ATTN: Open Source Program Office.