SecurID

RSA® Authentication Manager 8.7

Patch 3 Readme

March 2023

Contents

Before Installing This Patch

Note: All RSA Authentication Manager 8.7 patch releases are cumulative. You only need to apply the most recent patch to obtain all of the software fixes and updates that are included in the previous patches for version 8.7.

Before installing this patch, review the following guidelines:

- You must upgrade to RSA Authentication Manager 8.7 before installing this patch. For more information, see Upgrading RSA Authentication Manager on RSA Link.
- You must have at least 4 GB of free disk space to apply the patch.
- You must apply this patch to the primary instance before applying the patch to the replica instances in your deployment.
- If you have a replicated environment, all replica instances must be running and replicating successfully before you apply the patch to the primary or replica instances.
- 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.
- An updated web-tier server (available here) is also available with Patch 3. See the web-tier server Readme for information on these updates.

  You can use an Authentication Manager backup, Clonezilla for a hardware appliance, an Azure Snapshot or Backup, an AWS Snapshot, a VMware Snapshot or a Hyper-V Checkpoint.

Installing This Patch

The RSA Authentication Manager 8.7 Patch 3 ZIP file (**am-update-8.7.0.3.0.zip**) contains the RSA Authentication Manager 8.7 Patch 3 ISO file, **am-update-8.7.0.3.0.iso**, that is used to apply the patch to Authentication Manager.

Download and unzip the patch from RSA Link to a location that the primary or replica instance can access. You can apply an update through your web browser, or you can store patches in one of the following locations:

- NFS share
- Shared folder on Windows
- DVD/CD
- ISO image on your local machine.

The overall steps to install this patch are as follows:

- Specify a Product Update Location below
- Scan for Product Updates on the next page
- Apply Product Update on the next page

Specify a Product Update Location

To specify a product update location, perform the following procedure. This allows the RSA Authentication Manager 8.7 to locate patches. If you have already specified a location, see Scan for Product Updates on the next page.

Before You Begin

If you intend 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 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 from your local machine, select **Use your web browser to upload an update**. You do not need to scan for updates.
- If you want 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**
- If you want 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 and in the **Windows Password** field, enter a password only if it is required by your Windows share configuration.

- If you want 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 below.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, scan for product updates.

Scan for Product Updates

If you configured an update location, you can scan to locate and review a list of available product 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 patch to the RSA Authentication Manager deployment.

Apply Product Update

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

Before You Begin

- RSA recommends backing up your deployment before applying Patch 3. You can use an Authentication Manager backup, Clonezilla for a hardware appliance, an Azure Snapshot or Backup, an AWS Snapshot, a VMware Snapshot or a Hyper-V Checkpoint.

- 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.
- 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.

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 **Choose File** 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 **Update To Apply**, click **Apply Update**.

3. Check the update details, enter the password for the User ID **rsaadmin**, and 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 whether replication and RADIUS replication is functioning correctly on the primary instance and each replica instance.
- Patch 3 includes an updated web-tier server (available here). See the web-tier server Readme for information on these updates.

Rolling Back This Patch

When you roll back a patch, you remove the patch and all of the fixes included in the update. You can only remove the last patch 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 a patch.

Before You Begin

(VMware only) Patch 3 or later adds support for the VMXNET 3 and E1000E virtual network adapters for the VMware virtual appliance. If you have changed the default network adapter, you must do the following:

a. Manually add the E1000 virtual network adapter or connect the E1000 adapter if it is disconnected.

b. Delete the VMXNET 3 or E1000E virtual network adapter.

c. Reboot the virtual appliance.

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 an update is 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 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 appears.
- 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.

Next Steps

After you roll back Patch 3 on the primary and replica instances, you must reinstall the previous version of the web tier:

- Patch 3 includes an updated web tier version (available here).
- The version 8.7 web tier is included in the RSA Authentication Manager 8.7 Extras download kit (available here).

For instructions, see the "Reinstall the Web Tier" section of the RSA Authentication Manager 8.7 Setup and Configuration Guide.

If you restore the version 8.7 web tier, the web tier status remains as "Online, reinstall required." This message is displayed because the reinstalled web tier has an earlier version of WebLogic than the Authentication Manager instances. However, the functionality is not affected.

Secure Proxy and High Availability for DS100

From RSA Authentication Manager 8.7 onwards, the secure proxy and High Availability OTP features are available to the new RSA DS100 hardware authenticator. DS100 is a dual-use, cloud-managed hardware authenticator that can contain both a SecurID OTP authenticator and multiple FIDO authenticators. When deployed as a secure proxy server and failover node for the Cloud Authentication Service, Authentication Manager provides the secure proxy and High Availability OTP features to the SecurID OTP credentials only, not to the FIDO authenticators.

Defects Fixed in Patch 3

AM-46620: SameSite Flag is set to Strict mode for Session cookies console-selfservice-sp-session and console-selfservice-jsessionid.

AM-47758: SecurID RADIUS session ends once RADIUS Authentication is successful.

AM-47880: When the user name of the administrator doing token provisioning contains apostrophes, then searching of the closed requests by this user name would fail.

AM-46503: The wording in "Connect to Cloud Authentication Service" is not true where a customer is deploying an embedded identity router (IDR).

AM-48695: Updated SUSE components to fix issues reported by third parties.

AM-48694: Updated Oracle WebLogic components to fix various defects.

AM-48574: Extended the validation of Device Definition XML File for new Device Type in Software Token Profile.

AM-48887: All Users with Token report generated duplicate data when there are multiple custom user attributes are present causing increase in disk space.

Defects Fixed in Patch 2

RSA Authentication Manager 8.7 Patch 3 includes all fixes introduced in all versions 8.6 and 8.5 patches and security updates. In addition, the Patch 3 also contains fixes for the following issues.

AM-47675: Updated Oracle Weblogic and Java components to prevent vulnerability issues.

AM-47674: Updated SUSE Linux components used by RSA Authentication Manager to prevent potential security vulnerabilities.

AM-46898: AMBA UUD functions accurately if no token is assigned to the user for DefLogin.

AM-46286: Handling of the PIN history is now case sensitive.

Defects Fixed in Patch 1

AM-40671: The user gets locked out if the authentication fails repeatedly within a given time period after the first failed authentication.

AM-41590: On Authentication Manager, manual cronjob creation was not supported.

AM-44445: An error was displayed when an admin using the RSA Authentication Manager Security Console dashboard, assigned a token to a user who had an apostrophe (') in their user ID.

AM-45942: The configured DNS servers did not function accurately due to a network issue.

AM-46113: The Archive job displayed the number of rows purged and deleted accurately in the log.

AM-46400: All of the help choices for the CLU "manage-readonly-dbusers" are accurately displayed.

AM-46490: The RADIUS client statistics was not displayed to the user when it was accessed from the security console.

AM-46587: RADIUS shared secret value is validated when it is set in the RSA Authentication Manager Security Console or SDK.

AM-46762: Updated the Oracle WebLogic and Java components used by RSA Authentication Manager and web-tier to prevent potential security vulnerabilities.

AM-46763: Updated SUSE Linux components used by RSA Authentication Manager to prevent potential security vulnerabilities.

AM-47077: PIN + Approve or Biometrics authentication does not report an "Read cluster topology failure" error.

AM-47436: RADIUS authentication of double-byte Unicode characters in the username is successful.

Known Issues

Note: For SDK users - we are encouraging to use TLSv1.2 protocol in the client systems.

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 https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations 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.

March 2023

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.