RSA® Authentication Manager 8.3

Patch 3 Readme

September 2018

Prerequisite Release:
RSA Authentication Manager 8.3

Contents

Contents 1
Before Installing This Patch 1
Installing a Patch 2
Rolling Back This Patch 6
Upgrading to RSA Authentication Manager 8.3 7
New Features and Enhancements in Patch 3 7
New Features and Enhancements in Patch 2 7
New Features and Enhancements in Patch 1 8
Known Issues 9
Defects Fixed in This Patch 9
Support and Service 14

Before Installing This Patch

Note: All RSA Authentication Manager 8.3 patch releases are cumulative.

Before installing this patch, review the following guidelines:

- You must apply this patch to the primary and all replica instances in your RSA Authentication Manager 8.3 deployment. Make sure you apply the patch to the primary instance before applying the patch to the replica instances.
- 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. On the primary instance, the replication status displays “Internal Replication Error” or another error message until all replica instances have been upgraded or patched.
- You must have at least 4 GB of free disk space to apply the patch.
- You must upgrade a VMware virtual appliance or a hardware appliance to version 8.3 before installing this patch. See the *RSA Authentication Manager 8.3 Setup and Configuration Guide* for instructions.

Installing a Patch

The RSA Authentication Manager 8.3 Patch 3 ZIP file (**am-update-8.3.0.3.0.zip**) contains the RSA Authentication Manager 8.3 Patch 3 ISO file, **am-update-8.3.0.3.0.iso**, that is used to apply the patch 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 8.3 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**.

Note: If the update file is smaller than 2 GB, you can upload it through your local browser. If the size of the patch file exceeds 2 GB, however, you must change the update source settings and configure a new 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. If your Windows share configuration requires it, enter the domain and 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 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

- 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.

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**.

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 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.

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.

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.

Rolling back the patch results in the following:

- In the Operations Console, on the Update & Rollback page, the update no longer appears in the **Applied Updates** section.
- In the Security Console, the Software Version Information page no longer displays the patch number.

Upgrading to RSA Authentication Manager 8.3

RSA Authentication Manager 8.3 is a prerequisite release for this patch. Version 8.3 does not support direct migration from earlier versions. To use existing data from Authentication Manager 6.1, 7.1, or 8.0, do the following:

1. Deploy Authentication Manager 8.1 Service Pack 1. (8.1.1)
2. Migrate existing data from Authentication Manager 6.1, 7.1, or 8.0.
3. Update Authentication Manager 8.1.1 to version 8.3.
4. Install this patch.

New Features and Enhancements in Patch 3

Ability to Specify a Software Token Profile in AMBA

Distributing software tokens in RSA Authentication Manager 8.2 or later requires a software token profile. AMBA can specify a software token profile with the **SoftTokenProfile** attribute and define a global software token profile with the S**et Software Token Profile** (SSTP) command.

The software token profile allows AMBA to distribute software tokens with CT-KIP and SDTID files. AMBA does not support CTF.

For more information, see the *RSA Authentication Manager 8.3 Bulk Administration Utility (AMBA) Guide* on RSA Link at https://community.rsa.com/docs/DOC-86018.

Web Tier Qualification for RHEL 7.5

RSA has qualified the RSA Authentication Manager 8.3 Patch 3 web tier for compatibility with Red Hat Enterprise Linux 7.5.

New Features and Enhancements in Patch 2

Configure the Maximum Lifetime for New Emergency Access Tokencodes

You can use the new auth_manager.admin.eatokencode_expire_days global configuration value to set the maximum number of days that new Emergency Access Tokencodes can remain active. When a user or administrator activates a new Emergency Access Tokencode, they will not be allowed to set the expiration date later than the maximum lifetime you specify.

Procedure

Run the following command and then restart Authentication Manager services:

```
./rsautil store -a add_config auth_manager.admin.eatokencode_expire_days
days_value GLOBAL  501
```

where *days_value* is the maximum number of days that new Emergency Access Tokencodes can remain active.

New Features and Enhancements in Patch 1

Web Tier Qualification for Windows Server 2016 Standard

RSA has qualified the RSA Authentication Manager 8.3 Patch 1 web tier for compatibility with Windows Server 2016 Standard.

Known Issues

RSA Token Management Snap-In Help is Not Available
Tracking Number: AM-32316
Problem: If you try to access the RSA Token Management Snap-In Help, a "Page Not Found-404" error displays.

Workaround: All of the Help topics are available on RSA Link at https://community.rsa.com/docs/DOC-96830.

In some cases, after promoting a replica instance, the original (demoted) primary instance stops working.
Tracking Number: AM-32077
Problem: Sometimes, when promoting a replica instance to primary instance, the promotion succeeds, but the console displays a warning message, and services and synchronization on the original (demoted) primary instance stop working.

Workaround: Manually sign into the original (demoted) primary instance and start all Authentication Manager services, then resynchronize replication from the Operations Console on the new (promoted) primary instance.

Users cannot be added, disabled, or deleted from the Baseboard Management Controller interface on an Intel hardware appliance.
Tracking Number: AM-31722
Problem: A firmware problem prevents adding, disabling, and deletion of users from the Baseboard Management Controller (BMC) interface on certain Intel hardware appliances running BMC firmware prior to version 1.14.
Workaround: Download and install the latest BMC firmware package from Intel.

Defects Fixed in This Patch

8.3 Patch 3

Patch 3 contains fixes for the following issues:

AM-32194 – The versions of Oracle Java SE and WebLogic used by Authentication Manager and the web tier were potentially vulnerable to security exploits. If your deployment includes a web tier, you must reinstall the web tier with the latest version for this fix to work. See "Reinstall the Web Tier" in the *RSA Authentication Manager 8.3 Setup and Configuration Guide* for instructions. Release notes for the Authentication Manager 8.3 Patch 3 Web Tier Update are available on RSA Link.

AM-32184 – The latest expiration date allowed when activating new Emergency Access Tokencodes was one day earlier than the number of days specified by the eatokencode_expire_days global configuration value.

AM-32133 – Input validation for SearchGroupCommand and SearchGroupIterativeCommand incorrectly required a Group GUID value for searches that could be completed successfully if Group GUID was set as null.

AM-32132 – Operating system components used by Authentication Manager were vulnerable to several security exploits.

AM-32128 – The **view SecurID token demo** hyperlink in the Self-Service Console did not work.

AM-32022 – The online emergency access token count on the **Authentication > SecurID Tokens > Statistics** page of the Security Console incorrectly included tokens for which online emergency access had expired.

AM-31997 – In some cases, offline authentication did not work consistently for users with multiple tokens.

AM-31985 – The Security Console displayed a misleading success message after unsuccessful attempts to delete a user from the parent group of a nested subgroup.

AM-31981, AM-31982 – Elements of the Operations Console were vulnerable to Cross-Site Scripting (XSS) attacks.

AM-31978 – Authentication Manager instances where the Authentication Manager 8.3 upgrade kit was applied allowed anonymous and weak ciphers on ports for internal RADIUS operations.

AM-31947 – Some Authentication Manager console pages which previously included only the "no-cache" value in the HTTP cache-control response header will now also include "no-store".

AM-31894 – AMBA did not allow an administrator to assign a nickname to a token that had been unassigned from a user and reassigned to a different user.

AM-31745, AM-31677 – The Help documentation built into the Authentication Manager console pages was vulnerable to XSS attacks. If you use a language pack, you must download and install the latest language pack update for this fix to work.

AM-31737 – For the AMBA **Add Agent Host** (AAH) command, a Super Admin can use the new **AgentNewHostName** parameter to update the agent hostname.

AM-31395 – When revisiting the **Administration > Archive Audit Logs > Schedule Log Archival** page of the Security Console after selecting **Purge online log data stored for more than number of days specified below**, **Days Kept Online** was incorrectly displayed under the **Log Archival Export Directory** section.

AM-31056 – AMBA now includes a **SoftTokenProfile** attribute and a **Set Software Token Profile** (SSTP) command for software token distribution with CT-KIP and SDTID files. AMBA does not support CTF. For more information, see the *RSA Authentication Manager 8.3 Bulk Administration Utility (AMBA) Guide* on RSA Link at https://community.rsa.com/docs/DOC-86018.

AM-30999 – When editing an offline authentication policy in the Security Console, **Minimum Passcode Length** for offline authentication remained visible and editable when Enable Offline Authentication was disabled.

AM-18462 – Elements of the Security Console were vulnerable to XSS attacks.

8.3 Patch 2

Patch 2 contains fixes for the following issues:

AM-32062 – A planned promotion for the replica instance would fail during the promotion pre-check if the hostname for the primary instance used mixed-case characters.

AM-32009 – Administrators could not access Authentication Manager consoles by IP address after installing Patch 1.

AM-31984, AM-31973, AM-31956 – The versions of the SUSE Linux kernel, Oracle Java SE, Oracle WebLogic, and several other components used by Authentication Manager and the web tier were potentially vulnerable to security exploits. If your deployment includes a web tier, you must reinstall the web tier with the latest version for this fix to work. See "Reinstall the Web Tier" in the *RSA Authentication Manager 8.3 Setup and Configuration Guide* for instructions. Release notes for the Authentication Manager 8.3 Patch 2 Web Tier Update are available on RSA Link.

AM-31968, AM-31959 – Token lifetime extension did not work if the extension token randomly selected by Authentication Manager was previously returned to the unassigned token pool as the result of a token replacement operation.

AM-31881 – The procedure to remove the "view SecurID token demo" link from the Self-Service Console worked if the console was accessed directly through the Authentication Manager appliance, but did not remove the link from the web-tier Self-Service Console.

AM-31874/AM-31786 – Some characters in specific error messages were not displayed correctly in the German and Spanish localized versions of the Security Console.

AM-31501 – In some deployments, attempting to copy audit log entries did not succeed due to a signature mismatch error.

AM-31141 – Administrators lacked a method to control the maximum lifetime of Emergency Access Tokencodes. You can now set the maximum lifetime using a new global configuration value. For instructions, see Configure the Maximum Lifetime for Emergency Access Tokencodes.

AM-29080 – Administrators lacked the ability to rename RADIUS profiles after initially adding the profile and saving the settings for the first time. You can now rename profiles by editing the Profile Name field in the Security Console.

8.3 Patch 1

Patch 1 contains fixes for the following issues:

AM-32002 – The original version of Patch 1 that was published to RSA Link on May 3, 2018 did not install successfully on some Dell hardware appliances.

AM-31869 – The IPv4-IPv6 (TCP) Agent configuration interface accepted certificates with PEM encoding (as opposed to the expected DER encoding), which caused file corruption when generating **SDCONF.REC**.

AM-31868 – If an administrator entered an incorrect tokencode during RSA SecurID token resynchronization, the Security Console did not specify which of the two required tokencodes was invalid, and retrying the process caused significant delays. To address this issue, the Security Console now requests and validates each required tokencode individually.

AM-31867 – It was possible to import iOS CTKIP software tokens to Android devices, and vice versa.

AM-31834 – In some cases, a message indicating that a trusted realm relationship must be repaired appeared after the successful migration of an Authentication Manager 8.2 deployment for which no trusted realms were configured.

AM-31833 – Audit logs were not deleted from replica instances after being replicated to the primary instance, which caused disk space problems on the replica instances over time.

AM-31813 – The token expiration report ignored the token type filter and listed all tokens regardless of token type.

AM-31809 – In deployments where Authentication Manager was connected to the Cloud Authentication Service through an identity router, Authentication Manager stopped processing authentication requests over the REST interface if the identity router stopped responding.

AM-31796 – In specific network environments, Authentication Manager sometimes stopped responding to authentication requests on certain network ports, which prevented successful authentication until the server was restarted.

AM-31795 – The "Where do I find my serial number?" link in the Self-Service Console did not work on Internet Explorer or Chrome when the browser used a non-English language setting.

AM-31794 – Attempting to access the Self-Service Console Help from the Self-Service Console resulted in a 404 error.

AM-31793 – A time format mismatch caused connection errors and prevented successful integration between Authentication Manager and the Cloud Authentication Service if the identity router and the Authentication Manager instance were deployed in specific time zones.

AM-31790 – In some cases, attempting to view associated users for a RADIUS profile failed, triggering an error message.

AM-31789 – Archived logs were not stored under the **/opt/rsa/am/Log_archive** path as specified in the Security Console.

AM-31788 – When attempting to configure an IP address for a secondary network interface using the Security Console, the new IP address was set as the primary IP address, rather than the alternative IP address as expected.

AM-31787 – After installing Patch 5, importing users sometimes caused a DataNotFound error, and some users with replacement tokens were not imported as expected.

AM-31785 – Promotion and synchronization of replica instances did not succeed in certain environments where network latency and packet transmission problems caused SSL exceptions during data transfer.

AM-31783 – An administrator could inject control characters into the **/etc/hosts** file from the Operations Console which might have allowed the introduction of malicious data.

AM-31774 – In some cases, RADIUS services stopped responding and memory errors occurred when a WebLogic diagnostic file exceeded file size limitations.

AM-31767 – Operating system components used by Authentication Manager were vulnerable to several security exploits.

AM-31754 – The versions of Java and Oracle WebLogic used by Authentication Manager and the web tier were vulnerable to several security exploits. If your deployment includes a web tier, you must reinstall the web tier with the latest version for this fix to work. See "Reinstall the Web Tier" in the *RSA Authentication Manager 8.3 Setup and Configuration Guide* for instructions. Release notes for the Authentication Manager 8.3 Patch 1 Web Tier Update are available on RSA Link.

AM-31748 – A file on the Authentication Manager server was vulnerable to Cross-Site Scripting (XSS) attacks.

AM-31744 – The version of PopCalendarXP used by Authentication Manager was vulnerable to XSS attacks.

AM-31729 – Authentication Manager was vulnerable to XML External Entity (XXE) attacks from modified SecurID token job files imported to the Security Console.

AM-31714 – Authentication Manager did not boot if 8.2 SP1 Patch 4 or later was installed and rolled back, then a patch update lower than Patch 4 was installed.

AM-31583 – The "Low Token Supply" Critical System Event Notification did not trigger correctly when the token count matched the notification criteria.

AM-31578 – Input fields on the Dashboard page of the Security Console were vulnerable to Cross-Site Scripting (XSS) attacks.

AM-31439 – SecurID Authenticate tokens were incorrectly set to "next tokencode" mode in Authentication Manager after multiple unsuccessful authentication attempts.

AM-31304 – On-Demand Authentication (ODA) users were prompted to change their PIN after being exported and imported between Authentication Manager deployments.

AM-31234 – The "Identity Source Connection Failure" Critical Event Notification did not include the host name or IP address of the unresponsive identity source.

AM-30466 – A "TypeMismatchException" error appeared in the Authentication Manager system logs when searching for users that were present in more than one identity source, but not registered in the Authentication Manager database.

AM-29744 – Authentication Manager was vulnerable to a host header injection attack.

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.

September 2018

Trademarks

Intellectual Property Notice

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, EMC will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. EMC may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to EMC Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.